

LEARNING MADE EASY



5th Edition

CompTIA®

# A+® Certification

ALL-IN-ONE

for  
**dummies**®  
A Wiley Brand



**9**  
**Books**  
in one!

**PROCERT**  
CERTIFIED TRAINING

Glen E. Clarke  
Ed Tetz  
Timothy Warner



**This book comes with access to more content online.**

Watch videos, take practice tests,  
and study with flashcards!

Register your book or ebook at  
**[www.dummies.com/go/getaccess.](http://www.dummies.com/go/getaccess)**

Select your product, and then follow the prompts  
to validate your purchase.

You'll receive an email with your PIN and instructions.





# CompTIA® A+® Certification

ALL-IN-ONE

5th Edition

by Glen E. Clarke, Ed Tetz,  
and Timothy Warner

for  
**dummies**  
A Wiley Brand

# **CompTIA® A+® Certification All-in-One For Dummies®, 5th Edition**

Published by: **John Wiley & Sons, Inc.**, 111 River Street, Hoboken, NJ 07030-5774, [www.wiley.com](http://www.wiley.com)

Copyright © 2019 by John Wiley & Sons, Inc., Hoboken, New Jersey

Published simultaneously in Canada

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without the prior written permission of the Publisher. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at <http://www.wiley.com/go/permissions>.

**Trademarks:** Wiley, For Dummies, the Dummies Man logo, Dummies.com, Making Everything Easier, and related trade dress are trademarks or registered trademarks of John Wiley & Sons, Inc. and may not be used without written permission. CompTIA, A+, and the CompTIA Authorized Quality Curriculum logo are trademarks or registered trademarks of CompTIA Properties LLC. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc. is not associated with any product or vendor mentioned in this book.

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THE PUBLISHER AND THE AUTHOR MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES OR PROMOTIONAL MATERIALS. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY SITUATION. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT

ENGAGED IN RENDERING LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL SERVICES. IF PROFESSIONAL ASSISTANCE IS REQUIRED, THE SERVICES OF A COMPETENT PROFESSIONAL PERSON SHOULD BE SOUGHT. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. THE FACT THAT AN ORGANIZATION OR WEBSITE IS REFERRED TO IN THIS WORK AS A CITATION AND/OR A POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE AUTHOR OR THE PUBLISHER ENDORSES THE INFORMATION THE ORGANIZATION OR WEBSITE MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. FURTHER, READERS SHOULD BE AWARE THAT INTERNET WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ.

For general information on our other products and services, please contact our Customer Care Department within the U.S. at 877-762-2974, outside the U.S. at 317-572-3993, or fax 317-572-4002. For technical support, please visit

<https://hub.wiley.com/community/support/dummies>.

Wiley publishes in a variety of print and electronic formats and by print-on-demand. Some material included with standard print versions of this book may not be included in e-books or in print-on-demand. If this book refers to media such as a CD or DVD that is not included in the version you purchased, you may download this material at

<http://booksupport.wiley.com>. For more information about Wiley products, visit [www.wiley.com](http://www.wiley.com).

Library of Congress Control Number: 2019944088

ISBN 978-1-119-58106-2 (pbk); ISBN 978-1-119-58109-3 (ebk); ISBN 978-1-119-58108-6 (ebk)

# CompTIA Certification

## *It Pays to Get Certified*

**CompTIA** In a digital world, digital literacy is an essential survival skill. Certification proves you have the knowledge and skill to solve business problems in virtually any business environment. Certifications are highly valued credentials that qualify you for jobs, increased compensation, and promotion.



## *Certification Advances Your Career*



**The CompTIA A+ credential** provides foundation-level knowledge and skills necessary for a career in PC repair and support.

**Starting salary:** CompTIA A+ Certified individuals can earn as much as \$65,000 per year.

**Career pathway:** CompTIA A+ is a building block for other CompTIA certifications such as Network+, Security+, and vendor-specific

technologies.

**More than 850,000 individuals** worldwide are CompTIA A+ Certified.

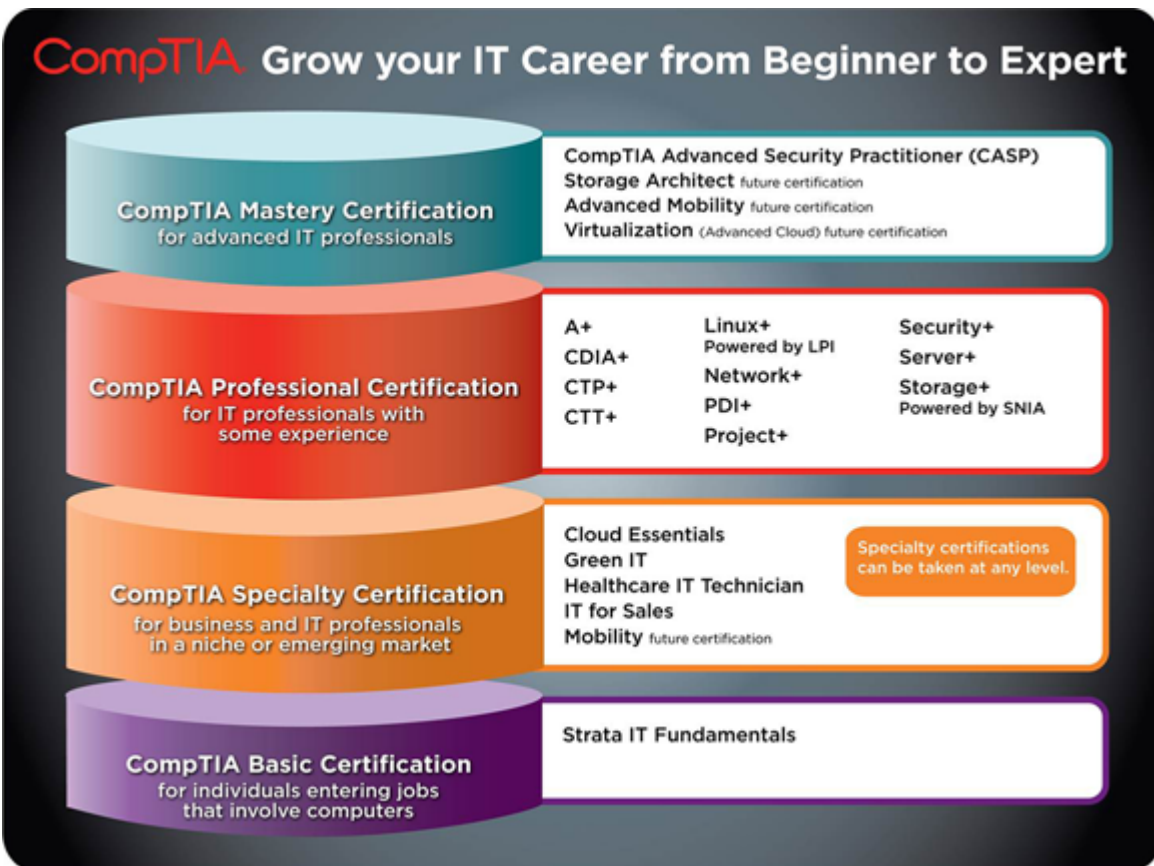
**Mandated/recommended by organizations worldwide** such as Cisco and HP and Ricoh, the U.S. State Department, and U.S. government contractors such as EDS, General Dynamics, and Northrop Grumman.

Some of the primary benefits individuals report from becoming A+ Certified are:

- » More efficient troubleshooting
- » Improved career advancement
- » More insightful problem solving

### ***CompTIA Career Pathway***

CompTIA offers a number of credentials that form a foundation for your career in technology and allow you to pursue specific areas of concentration. Depending on the path you choose to take, CompTIA certifications help you build upon your skills and knowledge, supporting learning throughout your entire career.



## Steps to Certification

### Steps to Getting Certified and Staying Certified

Review Exam Objectives	Review the certification objectives, located at <a href="https://certification.comptia.org/training/exam-objectives">https://certification.comptia.org/training/exam-objectives</a> , to make sure you know what is covered in the exam.
Practice for the Exam	After you have studied for the certification, take a free assessment and sample test to get an idea what type of questions might be on the exam at <a href="http://www.comptia.org/certifications/testprep/practicetests.aspx">http://www.comptia.org/certifications/testprep/practicetests.aspx</a> .
Purchase an Exam Voucher	Purchase your exam voucher on the CompTIA Marketplace, which is located at <a href="http://www.comptiastore.com">http://www.comptiastore.com</a> .
Take the Test!	Select a certification exam provider and schedule a time to take your exam. You can find exam providers at the following link: <a href="https://certification.comptia.org/testing/schedule-exam">https://certification.comptia.org/testing/schedule-exam</a> .

## Join the Professional Community

Join the IT Pro Community at <https://www.aitp.org>. The IT Pro online community provides valuable content to students and professionals.

» Career IT job resources

- Where to start in IT
- Career assessments
- Salary trends
- U.S. job board

» Forums on networking, security, computing and cutting-edge technologies

» Access to blogs written by industry experts

» Current information on cutting edge technologies

» Access to various industry resource links and articles related to IT and IT careers

## ***Why CompTIA?***

**Global Recognition:** CompTIA is recognized globally as the leading IT non-profit trade association and has enormous credibility. Plus, CompTIA's certifications are vendor-neutral and offer proof of foundational knowledge that translates across technologies.

**Valued by Hiring Managers:** Hiring managers value CompTIA certification because it is vendor and technology independent validation of your technical skills.

**Recommended or Required by Government and Businesses:** Many government organizations and corporations either recommend or require technical staff to be CompTIA certified (e.g., Dell, Sharp, Ricoh, the U.S. Department of Defense, and many more).

**Three CompTIA Certifications ranked in the top 10:** In a study by DICE of 17,000 technology professionals, certifications helped command higher salaries at all experience levels.

## ***How to Obtain More Information***

**Visit CompTIA online:** [www.comptia.org](http://www.comptia.org) to learn more about getting CompTIA certified.

**Contact CompTIA:** Call 866-835-8020 ext. 5 or email [questions@comptia.org](mailto:questions@comptia.org).



# CompTIA® A+® Certification All-in-One For Dummies®

To view this book's Cheat Sheet, simply go to [www.dummies.com](http://www.dummies.com) and search for “CompTIA A+ Certification All-In-One For Dummies Cheat Sheet” in the Search box.

## Table of Contents

### Cover

### Introduction

[About This Book](#)

[Conventions Used in This Book](#)

[Foolish Assumptions](#)

[How This Book Is Organized](#)

[Icons Used in This Book](#)

[Beyond the Book](#)

[Where to Go from Here](#)

### Pre-Assessment

[Questions](#)

[Answers](#)

### Book 1: Setting the A+ Groundwork

#### Chapter 1: The 2019 A+ Exams

[CompTIA A+ Certification and Why You Need It](#)

[Checking Out the Exams and Their Objectives](#)

[Using This Book to Prepare for the Exams](#)

[Making Arrangements to Take the Exams](#)

[The Day the Earth Stood Still: Exam Day](#)

## **Chapter 2: A+ Best Practices**

[Using Troubleshooting Procedures and Good Practices](#)

[Implementing Change Management](#)

[Professionalism and Communication](#)

[Getting an A+](#)

[Prep Test](#)

[Answers](#)

## **Chapter 3: Protecting Yourself and Your PC**

[Gathering Tools of the Trade](#)

[Avoiding the Dreaded ESD](#)

[Watching Out for EMI](#)

[Safety First!](#)

[Handling Toxic Waste](#)

[Environmental Impacts and Appropriate Controls](#)

[Exploring Ergonomics](#)

[Getting an A+](#)

[Prep Test](#)

[Answers](#)

## **Chapter 4: An Overview of System Components**

[What Is a Computer?](#)

[Looking Inside the Box](#)

[Checking Outside the Box](#)

[Getting an A+](#)

[Prep Test](#)

[Answers](#)

## **Book 2: Inside the Box**

### **Chapter 1: Knowing Your Motherboard**

[What's on the Front Panel](#)

[Finding Out What's on a Motherboard](#)

[Identifying the Types of Motherboards](#)

[Understanding Bus Architectures](#)

[Performance Considerations](#)

[Getting an A+](#)

[Prep Test](#)

[Answers](#)

## **Chapter 2: Picking Your Processor**

[Understanding Processor Terminology](#)

[Identifying Socket Types](#)

[Looking at Intel Processors](#)

[Don't Forget Non-Intel Chips](#)

[Installing a Processor](#)

[Keeping a Processor Cool](#)

[Increasing Performance](#)

[Getting an A+](#)

[Prep Test](#)

[Answers](#)

## **Chapter 3: What to Remember about Memory**

[Understanding the Types of Memory](#)

[Identifying the Types of DRAM](#)

[How Would You Like Your Chips Packaged?](#)

[Understanding Error-Checking Memory](#)

[Multichannel Memory Architecture](#)

[Single-Sided versus Double-Sided Memory](#)

[Buffered versus Unbuffered Memory](#)

[Working with Cache Memory](#)

[Installing or Upgrading Memory](#)

[Getting an A+](#)

[Prep Test](#)

[Answers](#)

## **Chapter 4: Telling Your BIOS from Your CMOS**

[BIOS versus CMOS](#)

[Upgrading the System BIOS/UEFI](#)

[Understanding CMOS](#)

[Viewing Basic Interface Settings](#)

[Viewing Advanced CMOS Settings](#)

[Getting an A+](#)

[Prep Test](#)

[Answers](#)

## **Chapter 5: Working with Storage**

[Understanding Hard Drive Terminology](#)

[Discovering IDE Devices](#)

[Learning How SCSI Works](#)

[Understanding Serial ATA](#)

[A Quick Tour of RAID](#)

[Using Removable Storage](#)

[Troubleshooting Hard Drives and RAID Arrays](#)

[Getting an A+](#)

[Prep Test](#)

[Answers](#)

## **Chapter 6: Working with Power**

[Knowing the Basics of Power Terminology](#)

[Identifying the Purpose of Power Supply Units](#)

[Identifying Power Supplies](#)

[Power Connectors](#)

[Power Supply Form Factors](#)

[Using AC Adapters](#)

[Working with UPS and Suppressors](#)

[Getting an A+](#)

[Prep Test](#)

[Answers](#)

## **Book 3: Outside the Box**

### **Chapter 1: Identifying Basic Cables and Connectors**

[Video Cables](#)

[Audio Cables and Connectors](#)

[Multipurpose Cables](#)

[Serial Cables](#)

[Hard Drive Cables](#)

[Adapters](#)

[Getting an A+](#)

[Prep Test](#)

[Answers](#)

## **Chapter 2: Installing and Configuring Input Devices**

[Minding Your Keys and Qs](#)

[Catching the Mouse](#)

[Communicating with Network Adapters](#)

[Other Input Devices](#)

[Getting an A+](#)

[Prep Test](#)

[Answers](#)

## **Chapter 3: Installing and Configuring Output Devices**

[Understanding Video Adapters](#)

[Using Your Monitor or Display](#)

[Troubleshooting Display Issues](#)

[The Sound of Computers](#)

[Other Output Devices](#)

[Getting an A+](#)

[Prep Test](#)

[Answers](#)

## **Chapter 4: Managing Printers**

[Learning about Paper Feeder Mechanisms](#)

[Understanding Types of Printers](#)

[Viewing Types of Printer Connections and Configurations](#)

[Upgrading Printer Hardware](#)

[Installing a Printer in Windows](#)

[Troubleshooting Printer Problems](#)

[Understanding Safety and Preventive Maintenance](#)

[Getting an A+](#)

[Prep Test](#)

[Answers](#)

## **Chapter 5: Working with Multimedia Devices**

[Understanding Scanners](#)

[Using Digital and Web Cameras](#)

[Looking at Other Multimedia Devices](#)

[Getting an A+](#)

[Prep Test](#)

[Answers](#)

## **Chapter 6: Dealing with Laptops and Mobile Devices**

[Identifying Portable Computer Components](#)

[Looking at Laptop Batteries](#)

[Understanding AC Adapters](#)

[Learning about LCD Panels](#)

[Understanding Laptop Input Devices](#)

[Laptop Communication Components](#)

[Port Replicators and Docking Stations](#)

[Expanding on a Laptop](#)

[Upgrading Your Laptop](#)

[Mobile Operating System Types](#)

[Troubleshooting Laptop Issues](#)

[Disassembling and Reassembling Laptops](#)

[Understanding Smartphones/Converged Devices](#)

[Securing Mobile Devices](#)

[Getting an A+](#)

[Prep Test](#)

[Answers](#)

## **Book 4: Maintenance and Troubleshooting**

### **Chapter 1: Performing Preventive Maintenance**

[Preventive Maintenance 101](#)

[Using Preventive Maintenance Tools](#)

[Maintaining Environmental Controls](#)

[Completing Maintenance Tasks](#)

[Getting an A+](#)

[Prep Test](#)

[Answers](#)

## **Chapter 2: Troubleshooting Procedures and Guidelines**

[The Art of Troubleshooting](#)

[Audio and Visual Troubleshooting](#)

[CMOS, BIOS, and UEFI](#)

[Hard Disk Drives and Solid State Drives](#)

[Optical Drives](#)

[Working with Connected Items](#)

[Power Supplies and Batteries](#)

[Getting an A+](#)

[Prep Test](#)

[Answers](#)

## **Book 5: Operating System Basics**

### **Chapter 1: System Design and Operating Systems**

[What Is an Operating System?](#)

[32-bit \(x86\) versus 64-bit \(x64\)](#)

[Looking at the Windows OS](#)

[Welcome to the Linux World](#)

[Understanding the Mac OS](#)

[Difference and Similarities between OSes](#)

[Choosing an Optimal System](#)

[Getting an A+](#)

[Prep Test](#)

[Answers](#)

### **Chapter 2: Windows Operating System Functions**

[Identifying Major Operating System Functions](#)

[Understanding Major Operating System Components](#)

[Navigating Your Computer](#)  
[Using Tools and Configuration Utilities](#)  
[Locating Major Files](#)  
[Examining Windows Features](#)  
[Virtualization Platforms](#)  
[Virtual Desktops](#)  
[Going to the Cloud](#)  
[Virtual Applications](#)  
[Getting an A+](#)  
[Prep Test](#)  
[Answers](#)

## **Chapter 3: Installing and Upgrading Windows**

[Understanding Installation Methods](#)  
[Preparing for Installation](#)  
[Performing Attended Installations of Windows](#)  
[Performing Unattended Installations of Windows](#)  
[Verifying and Troubleshooting the Installation](#)  
[Upgrading Windows](#)  
[Installing or Removing Additional Windows Components in Windows 10](#)  
[Restoring User Data Files](#)  
[Getting an A+](#)  
[Prep Test](#)  
[Answers](#)

## **Chapter 4: Managing Files and Directories**

[Identifying File-Naming Conventions](#)  
[Understanding File Attributes](#)  
[Getting an A+](#)  
[Prep Test](#)  
[Answers](#)

## **Chapter 5: Command Prompt Procedures**

[Using command.com and cmd.exe](#)  
[Executing Your Privileges](#)



[Managing Directories](#)

[Copying and Moving Files](#)

[Performing Diagnostics and Tuning Performance](#)

[Getting Active with Group Policy](#)

[Working with Other Useful Commands](#)

[Getting an A+](#)

[Prep Test](#)

[Answers](#)

## **Chapter 6: Working with System Files and the Boot Process**

[The Power-On Self-Test \(POST\) Process](#)

[Standard Boot Process for Windows](#)

[Managing Memory and Virtual Memory](#)

[Getting an A+](#)

[Prep Test](#)

[Answers](#)

## **Book 6: Managing the Operating System**

### **Chapter 1: Loading and Configuring Device Drivers**

[Loading Device Drivers](#)

[Changing Device Settings](#)

[Updating Drivers](#)

[Removing Device Drivers](#)

[Signed and Unsigned Drivers](#)

[Working with Plug and Play](#)

[Permissions to Install Drivers](#)

[Verifying Driver Installation](#)

[Device Driver Failure](#)

[Getting an A+](#)

[Prep Test](#)

[Answers](#)

### **Chapter 2: Working with Applications**

[Installing, Removing, and Repairing Applications](#)

[Getting the Most out of Multitasking](#)  
[Running 32-Bit and 64-Bit Windows Applications](#)  
[Running 16-Bit Windows Applications](#)  
[Running MS-DOS–Based Applications](#)  
[Windows Compatibility Modes](#)  
[Application Install, Start, and Load Errors](#)  
[Getting an A+](#)  
[Prep Test](#)  
[Answers](#)

### **Chapter 3: Optimizing the Windows Environment**

[Identifying Areas of System Bottlenecks](#)  
[Using Monitoring Tools](#)  
[Optimization Best Practices](#)  
[Getting an A+](#)  
[Prep Test](#)  
[Answers](#)

### **Chapter 4: Using Windows-Based Troubleshooting Utilities**

[Understanding Operating System Utilities for Disk Maintenance](#)  
[Working with Disk Management](#)  
[Configuration Utilities](#)  
[Getting a Handle on Diagnostic Utilities](#)  
[Miscellaneous Utilities](#)  
[Getting an A+](#)  
[Prep Test](#)  
[Answers](#)

### **Chapter 5: Scripting within the Operating System**

[Creating Your Files](#)  
[Going Back to Basics with Batch Files](#)  
[Working with VBScript](#)  
[Getting More Power with Windows PowerShell](#)  
[Shell \(.sh\) Script](#)

[Python Script](#)

[JavaScript](#)

[Commenting Your Code](#)

[Getting an A+](#)

[Prep Test](#)

[Answers](#)

## **Book 7: Recovering Systems**

### **Chapter 1: Managing Error Codes and Startup Messages**

[Windows Boot Files and Failure-to-Boot Errors](#)

[Solving Linux Boot Issues](#)

[Device-Related Errors](#)

[Other Errors](#)

[Error Diagnostic Tools](#)

[Getting an A+](#)

[Prep Test](#)

[Answers](#)

### **Chapter 2: Managing Common Problems**

[Solving Windows-Specific Service Problems](#)

[Solving Boot Errors and Errors Requiring Restarting](#)

[Resolving Device Driver and Service Errors](#)

[Application Install, Start, and Load Failures](#)

[Solving Linux File-Related Problems](#)

[Solving Other Problems](#)

[Getting an A+](#)

[Prep Test](#)

[Answers](#)

### **Chapter 3: Preparing for Disasters with Disaster Recovery**

[Using F8 Options during Boot-Up](#)

[Emergency Repair](#)

[Understanding Backup and Restore](#)

[Recovery and Rescue Methods](#)  
[Scheduling Preventive Maintenance](#)  
[Getting an A+](#)  
[Prep Test](#)  
[Answers](#)

## **Book 8: Networking**

### **Chapter 1: Down to the Networking Basics**

[Identifying the Types of Networks](#)  
[Understanding Network Topologies](#)  
[Connecting with Network Cabling](#)  
[Troubleshooting Networking Cables](#)  
[Examining Network Access Methods](#)  
[Piecing Together the Network Architectures](#)  
[Understanding Network Protocols](#)  
[Working with Network Devices](#)  
[Understanding Communication Methods](#)  
[Ways to Network a Computer](#)  
[Troubleshooting Networking Issues](#)  
[Getting an A+](#)  
[Prep Test](#)  
[Answers](#)

### **Chapter 2: Understanding Common Wireless Communications**

[Understanding Infrared Devices](#)  
[Working with Wireless Networks](#)  
[Installing and Configuring a SOHO Network](#)  
[Other Wireless Connections](#)  
[Increasing Wireless Network Performance](#)  
[Troubleshooting Issues](#)  
[Getting an A+](#)  
[Prep Test](#)  
[Answers](#)

## **Chapter 3: Networking the Operating System**

[Understanding Networking Components](#)

[The TCP/IP Protocol](#)

[VLANs](#)

[Understanding Name Resolution](#)

[Looking at Protocols and Ports](#)

[Troubleshooting with TCP/IP Utilities](#)

[Sharing File System Resources](#)

[Sharing Printer Resources](#)

[Networking with Windows](#)

[Understanding Windows Services](#)

[Getting an A+](#)

[Prep Test](#)

[Answers](#)

## **Chapter 4: Configuring Internet Access and SOHO Networks**

[Understanding the Internet](#)

[Using an ISP](#)

[Working with an ASP](#)

[Understanding Internet Protocols](#)

[Installing and Configuring Browsers](#)

[Using the Internet](#)

[Ways to Access the Internet](#)

[Installing a Small Office/Home Office \(SOHO\) Network](#)

[Firewalls and Home Routers](#)

[Getting an A+](#)

[Prep Test](#)

[Answers](#)

## **Book 9: Securing Systems**

### **Chapter 1: Fundamentals of Security**

[Identifying Types of Attacks](#)

[Understanding Physical Security](#)

[Understanding Authentication and Authorization](#)  
[Methods of Securing Transmissions](#)  
[Do Not Forget about Data Protection](#)  
[Prevention Methods and Best Practices](#)  
[Troubleshooting Mobile OS and Device Security](#)  
[Introduction to Incident Response](#)  
[Getting an A+](#)  
[Prep Test](#)  
[Answers](#)

## **Chapter 2: Implementing Security**

[Securing Systems through BIOS/UEFI](#)  
[Understanding Logical Security Concepts](#)  
[Implementing Users and Groups](#)  
[Implementing Permissions and Rights](#)  
[Implementing Auditing](#)  
[Implementing Firewalls](#)  
[Implementing Security Best Practices](#)  
[Getting an A+](#)  
[Prep Test](#)  
[Answers](#)

## **Chapter 3: Viruses and Malicious Software**

[My Computer Has a Virus!](#)  
[Understanding Malicious Software](#)  
[Identifying Hoaxes](#)  
[Preventing Problems by Staying Up to Date](#)  
[Recovering an Infected System](#)  
[Getting an A+](#)  
[Prep Test](#)  
[Answers](#)

## **Appendix A: CompTIA A+ Exam Reference Matrix**

[2019 Examination Objectives — 220-1001](#)  
[2019 Examination Objectives — 220-1002 Practical Application](#)

[Index](#)

[About the Authors](#)

[Connect with Dummies](#)

[End User License Agreement](#)

## List of Tables

### **Book 1 Chapter 1**

[TABLE 1-1 A+ Exam Information](#)

[TABLE 1-2 CompTIA A+ Exam \(220-1001\)](#)

[TABLE 1-3 CompTIA A+ Exam \(220-1002\)](#)

### **Book 1 Chapter 4**

[TABLE 4-1 Basic Types of Ports](#)

### **Book 2 Chapter 1**

[TABLE 1-1 PCMCIA Slot Types](#)

### **Book 2 Chapter 2**

[TABLE 2-1 Processor Socket Types and Slots](#)

[TABLE 2-2 Pentium Clock Multipliers](#)

### **Book 2 Chapter 3**

[TABLE 3-1 Identifying Memory Used by Your System](#)

### **Book 2 Chapter 4**

[TABLE 4-1 How to Enter CMOS Setup](#)

[TABLE 4-2 Parallel Port Mode](#)

### **Book 2 Chapter 5**

[TABLE 5-1 IDE versus EIDE](#)

[TABLE 5-2 PIO and DMA Modes](#)

[TABLE 5-3 Jumper Block Settings](#)

[TABLE 5-4 DVD Standards](#)

### **Book 2 Chapter 6**

[TABLE 6-1 Power Consumption by Product](#)

[TABLE 6-2 Pin Configuration for the Main Power Connector](#)

[TABLE 6-3 Pin Configuration for the Floppy Power Connector](#)

[TABLE 6-4 Pin Configuration for the Peripheral Power Connector](#)

[TABLE 6-5 Pin Configuration for the +12V2DC Power Connector](#)

[TABLE 6-6 Pin Configuration for the Serial ATA Power Connector](#)

[TABLE 6-7 6-Pin Configuration for the Serial ATA Power Connector](#)

[TABLE 6-8 8-Pin Configuration for the Serial ATA Power Connector](#)

## **Book 3 Chapter 1**

[TABLE 1-1 Types of Multimedia Connectors](#)

[TABLE 1-2 Serial Cable Pin Connections](#)

[TABLE 1-3 Null Modem Cable Pin Connections](#)

## **Book 3 Chapter 6**

[TABLE 6-1 Display Technologies](#)

## **Book 4 Chapter 1**

[TABLE 1-1 Shelf Life for Recorded and Stored Media](#)

## **Book 4 Chapter 2**

[TABLE 2-1 IBM POST Beep Codes](#)

## **Book 5 Chapter 1**

[TABLE 1-1 System Requirements for Microsoft Windows](#)

[TABLE 1-2 vi commands](#)

## **Book 5 Chapter 2**

[TABLE 2-1 OS Version Numbers for Modern Versions of Windows](#)

[TABLE 2-2 Differences between the Major Windows File Systems](#)

[TABLE 2-3 Control Panel Applets](#)

## **Book 5 Chapter 3**

[TABLE 3-1 Windows 10 Hardware Requirements](#)

## **Book 5 Chapter 4**

[TABLE 4-1 Directory Entry Format](#)

[TABLE 4-2 Short Filenames in Windows 7](#)

[TABLE 4-3 Executable File Extensions](#)

[TABLE 4-4 Application File Extensions](#)



[TABLE 4-5 Compression File Extensions](#)

[TABLE 4-6 System File Extensions](#)

[TABLE 4-7 Graphic File Extensions](#)

[TABLE 4-8 Miscellaneous File Extensions](#)

[TABLE 4-9 File Attributes](#)

[TABLE 4-10 Basic File Attributes](#)

[TABLE 4-11 compact.exe Command Switches](#)

[TABLE 4-12 cipher.exe Command Switches](#)

## **Book 5 Chapter 5**

[TABLE 5-1 Switches Used with the `runas` Command](#)

[TABLE 5-2 Ways to Specify Directory Paths](#)

[TABLE 5-3 Switches for `dir`](#)

[TABLE 5-4 Switches for `robocopy.exe`](#)

[TABLE 5-5 Switches for `shutdown.exe`](#)

[TABLE 5-6 Switches for `gpupdate`](#)

[TABLE 5-7 Switches for `gpresult`](#)

[TABLE 5-8 Switches for `dism.exe`](#)

## **Book 5 Chapter 6**

[TABLE 6-1 Device and Service Settings in the Registry](#)

## **Book 6 Chapter 3**

[TABLE 3-1 Related Objects for Critical System Resources](#)

[TABLE 3-2 Windows Services](#)

## **Book 6 Chapter 5**

[TABLE 5-1 Redirection Symbols](#)

[TABLE 5-2 Comparison Operators](#)

[TABLE 5-3 Boolean Operators](#)

[TABLE 5-4 Comment Syntax Symbols](#)

## **Book 8 Chapter 1**

[TABLE 1-1 UTP Category](#)

[TABLE 1-2 Types of Coax Cabling](#)

[TABLE 1-3 Project 802 LAN Standards](#)

[TABLE 1-4 The OSI Model](#)

## **Book 8 Chapter 3**

[TABLE 3-1 IP Address Classes](#)

[TABLE 3-2 Comparing IP Addresses with Subnet Mask](#)

[TABLE 3-3 IPCONFIG Switches](#)

[TABLE 3-4 Troubleshooting Network Connectivity](#)

[TABLE 3-5 NBTSTAT Switches](#)

[TABLE 3-6 NETSTAT Switches](#)

## **Book 8 Chapter 4**

[TABLE 4-1 Access Methods](#)

# List of Illustrations

## **Book 1 Chapter 2**

[FIGURE 2-1: Basic troubleshooting steps.](#)

## **Book 1 Chapter 3**

[FIGURE 3-1: A typical PC repair toolkit.](#)

[FIGURE 3-2: A digital multimeter can be a valuable tool when troubleshooting pow...](#)

[FIGURE 3-3: An antistatic wrist strap, also known as a grounding strap.](#)

[FIGURE 3-4: Having good posture when working on a computer helps prevent injurie...](#)

## **Book 1 Chapter 4**

[FIGURE 4-1: The major functions of the computer.](#)

## **Book 2 Chapter 1**

[FIGURE 1-1: A processor on a motherboard.](#)

[FIGURE 1-2: A ZIF socket on the motherboard.](#)

[FIGURE 1-3: DIMM memory slots on a motherboard.](#)

[FIGURE 1-4: L2 cache located on an older motherboard.](#)

[FIGURE 1-5: The relationship between the CPU and the motherboard chipset.](#)

[FIGURE 1-6: The North Bridge and South Bridge chips on an AOpen motherboard.](#)

[FIGURE 1-7: A BIOS chip located on the motherboard.](#)

[FIGURE 1-8: The battery \(on the motherboard\) used to maintain a charge to CMOS R...](#)

[FIGURE 1-9: Expansion slots \(PCI, PCIe 1x, and PCIe 16x\) on a motherboard.](#)

[FIGURE 1-10: Built-in ports on the back of an ATX motherboard.](#)

[FIGURE 1-11: Integrated ports on the back of an ATX motherboard.](#)

[FIGURE 1-12: A video adapter port.](#)

[FIGURE 1-13: How information flows from the processor to the display.](#)

[FIGURE 1-14: PS/2 connections for a keyboard and a mouse.](#)

[FIGURE 1-15: Sound ports on a system.](#)

[FIGURE 1-16: An RJ-45 port.](#)

[FIGURE 1-17: USB ports on the back of a motherboard.](#)

[FIGURE 1-18: A USB hub with four ports.](#)

[FIGURE 1-19: A digital video camera being connected to a system by the FireWire ...](#)

[FIGURE 1-20: Power connectors on an older motherboard.](#)

[FIGURE 1-21: The ATX power connector on an ATX motherboard.](#)

[FIGURE 1-22: 4-PIN and 6-PIN power connectors on an ATX motherboard.](#)

[FIGURE 1-23: EIDE connectors on the motherboard.](#)

[FIGURE 1-24: A 40-wire EIDE ribbon cable.](#)

[FIGURE 1-25: A SATA cable connected to the motherboard.](#)

[FIGURE 1-26: Identifying a jumper.](#)

[FIGURE 1-27: A DIP switch.](#)

[FIGURE 1-28: Looking at different motherboard form factors.](#)

[FIGURE 1-29: An NLX form factor motherboard.](#)

[FIGURE 1-30: The position of the I/O ports on an ATX motherboard.](#)

[FIGURE 1-31: The ATX motherboard is very popular in today's systems.](#)

[FIGURE 1-32: Compare ATX motherboard size \(left\) with a microATX motherboard \(ri...](#)

[FIGURE 1-33: Installing a card into a PCI slot on a motherboard.](#)

[FIGURE 1-34: A PCMCIA network card.](#)

[FIGURE 1-35: An AGP card in an AGP slot.](#)

[FIGURE 1-36: PCI Express slots on a motherboard.](#)

## **Book 2 Chapter 2**

[FIGURE 2-1: How system memory is organized.](#)

[FIGURE 2-2: Accessing two different memory addresses with the address bus.](#)

[FIGURE 2-3: Looking at the logical structure of a dual-core processor.](#)

[FIGURE 2-4: Comparing a DIP chip package \(right\) to a PGA package \(left\).](#)

[FIGURE 2-5: A ZIF socket on the motherboard holds a processor.](#)

[FIGURE 2-6: Intel processor and LGA socket.](#)

[FIGURE 2-7: An SEC chip package along with some PGA chip packages.](#)

[FIGURE 2-8: Identifying a processor socket.](#)

[FIGURE 2-9: Single-instruction pipelined processor executing application code.](#)

[FIGURE 2-10: Dual-instruction pipelined processor processing application code.](#)

[FIGURE 2-11: The Intel Pentium Pro processor.](#)

[FIGURE 2-12: Intel's Celeron processor was first implemented as an SEC package, ...](#)

[FIGURE 2-13: The Pentium III processor in the SEC2 package that lives in Slot 1.](#)

[FIGURE 2-14: The Pentium II Xeon processor was originally delivered in the SEC p...](#)

[FIGURE 2-15: Socket 478 can house a Pentium 4 processor.](#)

[FIGURE 2-16: Removing the processor from its socket.](#)

[FIGURE 2-17: The cut-out corner of the processor indicates the location of pin 1...](#)

[FIGURE 2-18: Identifying the cut-out corner in the processor socket.](#)

[FIGURE 2-19: Looking at a heat sink.](#)

[FIGURE 2-20: Placing the fan on top of the heat sink.](#)

## **Book 2 Chapter 3**

[FIGURE 3-1: Looking at how data is accessed in memory.](#)

[FIGURE 3-2: Viewing memory type with CPU-Z.](#)

[FIGURE 3-3: Looking at memory sockets on a motherboard.](#)

[FIGURE 3-4: Comparing a SODIMM and a DIMM.](#)

[FIGURE 3-5: Using CPU-Z to view memory channels.](#)

[FIGURE 3-6: How the CPU retrieves information from memory.](#)

[FIGURE 3-7: Viewing cache memory configuration.](#)

[FIGURE 3-8: Remove the cover to add memory to a laptop.](#)

[FIGURE 3-9: Inserting the SODIMM module into the memory slot.](#)

## **Book 2 Chapter 4**

[FIGURE 4-1: The BIOS chip \(an EEPROM chip located on the motherboard\) contains t...](#)

[FIGURE 4-2: Identifying the BIOS version by starting up the system.](#)

[FIGURE 4-3: The CMOS battery on the system board is responsible for powering CMO...](#)

[FIGURE 4-4: A typical CMOS screen.](#)

[FIGURE 4-5: Viewing the hard drive size in CMOS.](#)

[FIGURE 4-6: Changing the size of the floppy disk drive in CMOS.](#)

[FIGURE 4-7: Viewing the amount of memory installed on the system through CMOS.](#)

[FIGURE 4-8: Configuring the parallel port mode in CMOS.](#)

[FIGURE 4-9: Configuring the serial ports in CMOS.](#)

[FIGURE 4-10: Configuring the startup sequence in CMOS.](#)

[FIGURE 4-11: Setting an administrator password in CMOS.](#)

[FIGURE 4-12: A jumper that can be removed to erase the CMOS password.](#)

[FIGURE 4-13: Viewing the system UUID and BIOS revision number through CMOS.](#)

[FIGURE 4-14: Disabling USB ports prevents using flash drives or other USB-type d...](#)

[FIGURE 4-15: Viewing the virus protection setting in CMOS.](#)

[FIGURE 4-16: Disable built-in cache memory in CMOS to troubleshoot problems with...](#)

[FIGURE 4-17: Enabling virtualization support in order to use VMs.](#)

[FIGURE 4-18: Performing memory diagnostics.](#)

[FIGURE 4-19: Changing AHCI mode in CMOS.](#)

## **Book 2 Chapter 5**

[FIGURE 5-1: The internals of a hard disk.](#)

[FIGURE 5-2: Sides of a platter.](#)

[FIGURE 5-3: Tracks and sectors on a disk platter.](#)

[FIGURE 5-4: Measuring seek time.](#)

[FIGURE 5-5: Mounting the hard disk into the drive bay.](#)

[FIGURE 5-6: An IDE ribbon cable.](#)

[FIGURE 5-7: Connecting an IDE drive.](#)

[FIGURE 5-8: One drive is configured as the master, and the other is configured a...](#)

[FIGURE 5-9: Adjust the jumpers to set one drive as a master and the other as a s...](#)

[FIGURE 5-10: Looking at an additional jumper configuration for a dual-drive setu...](#)

[FIGURE 5-11: The SCSI host adapter.](#)

[FIGURE 5-12: Looking at a SCSI daisy chain.](#)

[FIGURE 5-13: Assigning a SCSI ID to an external device.](#)

[FIGURE 5-14: Looking at internal SCSI connectors.](#)

[FIGURE 5-15: Looking at external SCSI connectors.](#)

[FIGURE 5-16: A SCSI terminator.](#)

[FIGURE 5-17: An LVD SCSI card with hard drive and internal cable.](#)

[FIGURE 5-18: A SATA cable and power connector connecting to a SATA drive.](#)

[FIGURE 5-19: An eSATA connector on an external hard drive.](#)

[FIGURE 5-20: A flash drive uses a USB connection to interface with the computer.](#)

[FIGURE 5-21: A CompactFlash, SD card, and SD card carry case.](#)

## **Book 2 Chapter 6**

[FIGURE 6-1: Power connectors that may be used on power supplies.](#)

[FIGURE 6-2: Power supply unit form factors.](#)

[FIGURE 6-3: Front and rear of a standard server UPS.](#)

## **Book 3 Chapter 1**

[FIGURE 1-1: A docking station with a variety of video interfaces.](#)

[FIGURE 1-2: DVI connector variants.](#)

[FIGURE 1-3: Thunderbolt USB-C connectors. Note the Thunderbolt icon on the left ...](#)

[FIGURE 1-4: A sample of the most common USB connectors.](#)

[FIGURE 1-5: The DB-9 connector.](#)

[FIGURE 1-6: The DB-25 connector.](#)

[FIGURE 1-7: Ribbon cable used for IDE/ATA connections.](#)

[FIGURE 1-8: SATA and eSATA connectors.](#)

[FIGURE 1-9: USB to Ethernet; DisplayPort to VGA, HDMI, and DVI; and two DVI to V...](#)

## **Book 3 Chapter 2**

[FIGURE 2-1: The five major keyboard key groupings.](#)

[FIGURE 2-2: A natural, ergonomic-style keyboard.](#)

[FIGURE 2-3: Change keyboard properties through the Windows 10 Control Panel.](#)

[FIGURE 2-4: Change the keyboard accessibility options in Windows 10.](#)

[FIGURE 2-5: As the mouse moves, the holes and solid areas of the encoding disc h...](#)

[FIGURE 2-6: Installing a PCI network card into the PCI slot of a computer.](#)

[FIGURE 2-7: Configuring network card settings through Windows Device Manager in ...](#)

[FIGURE 2-8: A touch pad is a popular input device to control the mouse pointer o...](#)

## **Book 3 Chapter 3**

[FIGURE 3-1: Looking at the back of a video card and the port style.](#)

[FIGURE 3-2: An HDMI connector \(top left\), a DVI connector \(top right\), and an HD...](#)

[FIGURE 3-3: Configuring sound settings in Windows 10.](#)

## **Book 3 Chapter 4**

[FIGURE 4-1: Looking at a laser printer.](#)

[FIGURE 4-2: A toner cartridge found in laser printers.](#)

[FIGURE 4-3: Identifying the laser printing process.](#)

[FIGURE 4-4: An inkjet printer.](#)

[FIGURE 4-5: A USB connector is a popular method today to connect printers to com...](#)

[FIGURE 4-6: Installing a local printer in Windows 10.](#)

[FIGURE 4-7: The priority setting and the scheduling option on a printer.](#)

[FIGURE 4-8: Sharing a printer.](#)

[FIGURE 4-9: The Print Management console is a great Windows 10 tool that unifies...](#)

[FIGURE 4-10: Editing the spooler services properties on a Windows system.](#)

[FIGURE 4-11: Changing the spooling folder on a Windows 10 system.](#)

[FIGURE 4-12: Managing a single print job within the print queue.](#)

[FIGURE 4-13: Managing the print queue.](#)

## **Book 3 Chapter 5**

[FIGURE 5-1: A flatbed scanner uses a scan head that moves under the object being...](#)

[FIGURE 5-2: Webcam-enabled applications like Skype let you chat or video confere...](#)

[FIGURE 5-3: A webcam captures live video and sends it to anyone you are conferen...](#)

[FIGURE 5-4: Managing recording and playback devices in Windows 10.](#)

[FIGURE 5-5: Ensure the microphone is set as a recordable device.](#)

[FIGURE 5-6: Use a TV tuner card to receive a TV signal on a computer.](#)

## **Book 3 Chapter 6**

[FIGURE 6-1: Identifying the major components of a portable computer.](#)

[FIGURE 6-2: Replacing a battery on a laptop system.](#)

[FIGURE 6-3: Configuring sleep timers in Windows 10.](#)

[FIGURE 6-4: Choose the Sleep option from the Start menu in Windows 10.](#)

[FIGURE 6-5: An AC adapter supplies power to the laptop and charges the battery.](#)

[FIGURE 6-6: Use a touch pad to move the mouse pointer.](#)

[FIGURE 6-7: SODIMM slots on the laptop to allow more memory to be added to the l...](#)

[FIGURE 6-8: Replace the hard drive on a laptop for more storage.](#)

[FIGURE 6-9: Add storage space by using a USB external hard drive \(top\) or a USB ...](#)

[FIGURE 6-10: Most laptops have a built-in number pad that you activate with the ...](#)

[FIGURE 6-11: A collection of current handheld devices.](#)

## **Book 4 Chapter 1**

[FIGURE 1-1: Typical airflow in a tower case. The darker the arrow, the warmer th...](#)

## **Book 4 Chapter 2**

[FIGURE 2-1: Some of these capacitors have damage. Note the residue on the top of...](#)



[FIGURE 2-2: Some drives have multiple jumper configurations for the same setting...](#)

[FIGURE 2-3: Keyboards can be taken apart and cleaned, but they do contain a lot ...](#)

[FIGURE 2-4: Here is a device powered by two USB ports, using a pass-through conn...](#)

[FIGURE 2-5: A power supply tester can save time when testing voltage supplied by...](#)

[FIGURE 2-6: Back-probing power connectors is a standard method for testing power...](#)

## **Book 5 Chapter 1**

[FIGURE 1-1: The Windows 8.1 GUI.](#)

[FIGURE 1-2: The Windows 7 desktop.](#)

[FIGURE 1-3: The Windows 8.1 desktop.](#)

[FIGURE 1-4: The Windows 10 desktop.](#)

[FIGURE 1-5: The GNOME desktop environment in action.](#)

[FIGURE 1-6: The Macintosh GUI for macOS.](#)

## **Book 5 Chapter 2**

[FIGURE 2-1: The System Control Panel is available in all versions of Windows.](#)

[FIGURE 2-2: The System Information tool for Windows provides a great deal of det...](#)

[FIGURE 2-3: The Windows architectural overview.](#)

[FIGURE 2-4: A sample of virtual memory within the Windows 8.1 OS.](#)

[FIGURE 2-5: Use This PC or Computer to navigate file systems on the drive.](#)

[FIGURE 2-6: A Remote Desktop Connection to another computer on the network.](#)

[FIGURE 2-7: The Remote Assistance process can be a boon for many help desk perso...](#)

[FIGURE 2-8: A comparison of cloud services and management responsibility.](#)

## **Book 5 Chapter 3**

[FIGURE 3-1: Installing Windows 10 has never been easier to do.](#)

[FIGURE 3-2: Activating Windows 10 in the Settings panel.](#)

[FIGURE 3-3: Use Windows System Image Manager \(SIM\) to create an unattended answe...](#)

[FIGURE 3-4: Installing additional Windows components in Windows 10.](#)

[FIGURE 3-5: Installing additional Windows components in Windows 10.](#)

## **Book 5 Chapter 4**

[FIGURE 4-1: Each file has an icon that represents its file association.](#)

[FIGURE 4-2: You can create file associations in the Open With dialog box.](#)

[FIGURE 4-3: Windows 7 offers to locate the application required to work with a f...](#)

[FIGURE 4-4: Changing the file type association using Default Programs on Windows...](#)

[FIGURE 4-5: You can tweak your Folder Options to display file extensions on your...](#)

[FIGURE 4-6: The Compress attribute is set on a file-by-file or folder basis.](#)

[FIGURE 4-7: You can grant other users access to your encrypted files.](#)

[FIGURE 4-8: Indexing can be enabled for your whole drive or for just a folder.](#)

[FIGURE 4-9: You must have folders included in the index to be able to search by...](#)

[FIGURE 4-10: On NTFS partitions, you see only the Read-only and Hidden attribute...](#)

[FIGURE 4-11: The Advanced Attributes window is available only on NTFS partitions...](#)

## **Book 5 Chapter 6**

[FIGURE 6-1: The swap process.](#)

## **Book 6 Chapter 1**

[FIGURE 1-1: Using Windows Update for drivers can make it extremely easy to deal ...](#)

[FIGURE 1-2: Plug and Play detection is used to initially locate all devices on y...](#)

[FIGURE 1-3: Choose the type of device you are installing so that you can look at...](#)

[FIGURE 1-4: Device lists are listed by manufacturer to make locating devices eas...](#)

[FIGURE 1-5: You might have to tell Windows what resources your device requires.](#)

[FIGURE 1-6: Device Manager is a powerful tool when it comes to device management...](#)

[FIGURE 1-7: Driver signing prevents installation of unwanted drivers.](#)

[FIGURE 1-8: The Plug and Play concept is very simple in design.](#)

[FIGURE 1-9: The Local Security Policy allows you to install device drivers.](#)

## **Book 6 Chapter 2**

[FIGURE 2-1: The Uninstall options in Windows are more streamlined than previous ...](#)

[FIGURE 2-2: 32-bit applications run in their own execution area in Windows.](#)

[FIGURE 2-3: In 64-bit Windows, 32-bit applications run through an emulation layer...](#)

[FIGURE 2-4: PIFs have several tabs that contain settings for a simulated MS-DOS ...](#)

[FIGURE 2-5: Each PIF for a common application can contain unique settings.](#)

[FIGURE 2-6: The Compatibility settings for an application.](#)

## **Book 6 Chapter 3**

[FIGURE 3-1: The Performance tab of Task Manager is usually the first place to lo...](#)

[FIGURE 3-2: Resource Monitor shows detailed information related to processes.](#)

[FIGURE 3-3: Windows 8.1 enhances the information displayed on the Performance ta...](#)

[FIGURE 3-4: The Processes tab of Task Manager helps identify CPU utilization pro...](#)

[FIGURE 3-5: The Applications tab lists running foreground applications and their...](#)

[FIGURE 3-6: Performance Monitor shows graphs for a variety of counters built int...](#)

[FIGURE 3-7: A wide variety of counters may be added to your graph.](#)

[FIGURE 3-8: Add counters and set alert thresholds.](#)

[FIGURE 3-9: Set alerts to notify you of problem conditions.](#)

[FIGURE 3-10: Performance counter logs can be used to record data for historical ...](#)

[FIGURE 3-11: Resource Monitor will show data regarding all four resource categor...](#)

[FIGURE 3-12: CPU data will identify issues with processes or applications that a...](#)

[FIGURE 3-13: Memory statistics will identify memory consumption issues.](#)

[FIGURE 3-14: Disk activity identified by process.](#)

[FIGURE 3-15: Network activity can be viewed in great detail.](#)

[FIGURE 3-16: Changing the page file settings can improve your overall system per...](#)

[FIGURE 3-17: Changing the spool folder path may improve printing performance.](#)

## **Book 6 Chapter 4**

[FIGURE 4-1: Disk Management is more user-friendly than `diskpart.exe`](#)

[FIGURE 4-2: You have two interfaces to choose from to defragment your drives.](#)

[FIGURE 4-3: Standard scans check the structure of the file tables.](#)

[FIGURE 4-4: Assigning drive letters with Disk Management.](#)

[FIGURE 4-5: Disk initialization with Disk Management.](#)

[FIGURE 4-6: Extending a partition with Disk Management.](#)

[FIGURE 4-7: Storage Spaces provides storage flexibility.](#)

[FIGURE 4-8: Creating a new volume using Windows 10 Storage Spaces.](#)

[FIGURE 4-9: The initial window for System Configuration allows you to modify the...](#)

[FIGURE 4-10: Settings in the Registry cover most aspects of the system.](#)

[FIGURE 4-11: There are six basic data types for the Windows Registry.](#)

[FIGURE 4-12: Export sections of the Registry as backup prior to editing.](#)

[FIGURE 4-13: All Registry export files share a structure that resembles Windows ...](#)

[FIGURE 4-14: Heed the confirmation to limit accidental imports.](#)

[FIGURE 4-15: A successful Registry import.](#)

[FIGURE 4-16: When looking for malfunctioning devices, look for the warning symbol...](#)

[FIGURE 4-17: Computer Management is your one-stop shop for system management uti...](#)

[FIGURE 4-18: The System Information tool provides information about your install...](#)

[FIGURE 4-19: The System log has several types of messages telling you about majo...](#)

[FIGURE 4-20: The detailed information for an event gives you several relevant pi...](#)

[FIGURE 4-21: Windows Memory Diagnostics is a special command screen that operate...](#)

[FIGURE 4-22: DirectX Diagnostics gives you a quick snapshot of the DirectX drive...](#)

[FIGURE 4-23: Data Sources allows you to manage database connections.](#)

[FIGURE 4-24: When adding snap-ins to MMC, you can often target another computer.](#)

## **Book 7 Chapter 1**

[FIGURE 1-1: Ubuntu Linux is known for being simple to use. Even re-installing th...](#)

[FIGURE 1-2: Type \*\*msconfig\*\* from a Windows command prompt to open the System Confi...](#)

[FIGURE 1-3: Windows Error Reporting helps Microsoft fix problems with the OS.](#)

[FIGURE 1-4: Even with Error Reporting enabled, you can control what errors go to...](#)

[FIGURE 1-5: The default settings for the Windows 8.1 and Windows 10- log files w...](#)

## **Book 7 Chapter 2**

[FIGURE 2-1: Restarting services is easy from the Services Administrative tool.](#)

[FIGURE 2-2: Auto-restarting a service after a failure is just one of the options...](#)

[FIGURE 2-3: Stop errors are “affectionately” known as the Blue Screen of Death.](#)

[FIGURE 2-4: Windows 10 gives you a 21st century, emoticon-friendly stop message.](#)

[FIGURE 2-5: The “Spinning Beach Ball of Death” and the kernel panic \(system cras...](#)

[FIGURE 2-6: You’ll see the Windows Error Recovery screen if your system was shut...](#)

[FIGURE 2-7: Press Ctrl+Alt+Del in Windows 8.1 or Windows 10 to access Task Manag...](#)

[FIGURE 2-8: The Processes tab in the Windows 10 Task Manager enables you to view...](#)

[FIGURE 2-9: You can run applications in compatibility mode if they don’t run cor...](#)

[FIGURE 2-10: You set file associations in Ubuntu the same way you do so in Windo...](#)

[FIGURE 2-11: Modern UEFI systems normally include rich diagnostics to help you e...](#)

## **Book 7 Chapter 3**

[FIGURE 3-1: Safe Mode should be easy to spot, with the wording in each corner.](#)

[FIGURE 3-2: Get ready to enter the Windows Recovery Environment in Windows 10.](#)

[FIGURE 3-3: Windows RE allows you to refresh, reset, or troubleshoot a Windows 8...](#)

[FIGURE 3-4: The Advanced Options screen gives you access to the core Windows rec...](#)

[FIGURE 3-5: Creating a system recovery image in Windows 8.1.](#)

[FIGURE 3-6: Restoring a System Recovery Image in Windows 8.1.](#)

[FIGURE 3-7: The Windows 7 Backup and Restore tool is wizard-based and intuitive ...](#)

[FIGURE 3-8: File History automates the backup of user data in Windows 8.1 and Wi...](#)

[FIGURE 3-9: Restoring missing personal files by using File History is simple.](#)

[FIGURE 3-10: PC Refresh and Reset are two valuable Windows 8.1 tools for any A+ ...](#)

[FIGURE 3-11: The System Restore Wizard in Windows 8.1 and Windows 10.](#)

[FIGURE 3-12: Changing the System Restore cache size.](#)

[FIGURE 3-13: If your computer has unique hardware, you might need to use special...](#)

[FIGURE 3-14: Local files can be managed and many settings viewed.](#)

[FIGURE 3-15: The disk partition management is easy to use after you understand h...](#)

[FIGURE 3-16: Files may be transferred to and from file servers.](#)

## **Book 8 Chapter 1**

[FIGURE 1-1: Peer-to-peer network environments.](#)

[FIGURE 1-2: Server-based networking environment.](#)

[FIGURE 1-3: A bus topology.](#)

[FIGURE 1-4: A star topology.](#)

[FIGURE 1-5: A hybrid topology.](#)

[FIGURE 1-6: A wireless network topology.](#)

[FIGURE 1-7: Unshielded twisted pair cabling.](#)

[FIGURE 1-8: Shielded twisted pair cabling.](#)

[FIGURE 1-9: An RJ-45 connector \(left\) and an RJ-11 connector \(right\).](#)

[FIGURE 1-10: Looking at coaxial cable and a coax cable with the BNC style connec...](#)

[FIGURE 1-11: An F-type connector and a BNC connector.](#)

[FIGURE 1-12: A BNC connector connecting to a workstation.](#)

[FIGURE 1-13: A BNC-T connector used on Thinnet coax cable.](#)

[FIGURE 1-14: A BNC-T connector with a terminator.](#)

[FIGURE 1-15: An AUI port.](#)

[FIGURE 1-16: Fiber optic cabling.](#)

[FIGURE 1-17: Looking at strands in fiber optic cabling along with the SC \(bottom...](#)

[FIGURE 1-18: A network interface card.](#)

[FIGURE 1-19: A repeater is used to regenerate the signal.](#)

[FIGURE 1-20: A bridge forwards network traffic to only the destination segment.](#)

[FIGURE 1-21: Routers send data from one network to another.](#)

[FIGURE 1-22: A network hub with eight RJ-45 ports and one BNC port.](#)

[FIGURE 1-23: A 24-port network switch.](#)

[FIGURE 1-24: A four-port wireless router also contains a WAN link for the Intern...](#)

## **Book 8 Chapter 2**

[FIGURE 2-1: Wireless networks are usually run in infrastructure mode but can als...](#)

[FIGURE 2-2: Windows wireless settings are accessed via the Network and Sharing C...](#)

[FIGURE 2-3: Normal channel frequencies used for 802.11b/g networks.](#)

[FIGURE 2-4: Security options for a typical wireless access point.](#)

[FIGURE 2-5: Changing the SSID and disabling SSID broadcasting.](#)

[FIGURE 2-6: Configuring DHCP.](#)

[FIGURE 2-7: Changing the admin password.](#)

[FIGURE 2-8: Configuring wireless encryption.](#)

[FIGURE 2-9: Configuring MAC filtering.](#)

[FIGURE 2-10: Use Acrylic WiFi scanner and similar tools to see wireless networks...](#)

## **Book 8 Chapter 3**

[FIGURE 3-1: The relationship between the OS and a hardware device is controlled ...](#)

[FIGURE 3-2: Updating a network card driver in Windows.](#)

[FIGURE 3-3: Viewing local area connection in Windows.](#)

[FIGURE 3-4: Verify that Client for Microsoft Networks is installed.](#)

[FIGURE 3-5: Configuring TCP/IP on a Windows client.](#)

[FIGURE 3-6: Configuring Windows as a DHCP client.](#)

[FIGURE 3-7: Changing your computer name in Windows.](#)

[FIGURE 3-8: Configuring a WINS client in Windows.](#)

[FIGURE 3-9: An example of an `LMHOSTS` file in Windows.](#)

[FIGURE 3-10: Configuring a Windows client for DNS.](#)

[FIGURE 3-11: An example of a `HOSTS` file used for FQDN resolution.](#)

[FIGURE 3-12: Punchdown tool \(left\) and crimper \(right\).](#)

[FIGURE 3-13: Verifying that File and Printer Sharing is installed on Windows.](#)

[FIGURE 3-14: Sharing a folder.](#)

[FIGURE 3-15: Assigning permissions levels in Windows.](#)

[FIGURE 3-16: Mapping a network drive in Windows.](#)

[FIGURE 3-17: Network and Sharing Center window in Windows.](#)

[FIGURE 3-18: Configuring a homegroup.](#)

[FIGURE 3-19: Advanced sharing settings.](#)

## **Book 8 Chapter 4**

[FIGURE 4-1: How you connect to the Internet.](#)

[FIGURE 4-2: TCP/IP uses many protocols at different layers to accomplish its tas...](#)

[FIGURE 4-3: Where mail protocols are used.](#)

[FIGURE 4-4: Configuring SMTP and POP3 server settings.](#)

[FIGURE 4-5: Web browsers let you retrieve data from a server using HTTP.](#)

[FIGURE 4-6: Choosing the right client for the job is important.](#)

[FIGURE 4-7: Manage web browser settings through Internet Options.](#)

[FIGURE 4-8: Security settings in Internet Explorer can make the browser much saf...](#)



[FIGURE 4-9: If you are using proxy settings, you might need to regularly enable ...](#)

[FIGURE 4-10: Security Settings are just one of the types of Advanced Settings.](#)

[FIGURE 4-11: Overview of the domain name system.](#)

[FIGURE 4-12: Configuring a wireless hotspot on an iPhone.](#)

[FIGURE 4-13: Typical firewall settings on a home router.](#)

## **Book 9 Chapter 1**

[FIGURE 1-1: Cracking passwords with LC4.](#)

[FIGURE 1-2: Using Network Monitor to analyze FTP logon traffic.](#)

[FIGURE 1-3: Using NetBus to control a user's computer.](#)

[FIGURE 1-4: Enabling the BIOS password.](#)

[FIGURE 1-5: A lockdown cable is used to secure computer equipment to a desk.](#)

[FIGURE 1-6: A fingerprint reader is an example of biometrics used for authentica...](#)

[FIGURE 1-7: Logging on to Active Directory in a Microsoft network environment.](#)

[FIGURE 1-8: Using permissions to authorize which users are allowed to access the...](#)

[FIGURE 1-9: Identifying a secure site by locating the lock in Internet Explorer.](#)

[FIGURE 1-10: Viewing the archive bit in Windows.](#)

## **Book 9 Chapter 2**

[FIGURE 2-1: Creating user accounts and groups in the Computer Management console...](#)

[FIGURE 2-2: Creating a user account in Windows.](#)

[FIGURE 2-3: Creating a user account via Control Panel.](#)

[FIGURE 2-4: Creating a new group in Computer Management.](#)

[FIGURE 2-5: Fill in information for your new group.](#)

[FIGURE 2-6: Configuring user rights within Windows allows you to control which a...](#)

[FIGURE 2-7: Adding Bob to the change the system time user right.](#)

[FIGURE 2-8: Modifying the UAC feature within the Local Security Policy.](#)

[FIGURE 2-9: Modifying the UAC feature via Control Panel.](#)

[FIGURE 2-10: Looking at NTFS permissions in Windows.](#)

[FIGURE 2-11: Disabling permission inheritance in the Advanced Security Settings ...](#)

[FIGURE 2-12: Giving the accountants the Modify permission.](#)

[FIGURE 2-13: Looking at the auditing feature within the Local Security Policy.](#)

[FIGURE 2-14: Review the security log that is populated by the auditing feature o...](#)

[FIGURE 2-15: The Windows Firewall in Control Panel.](#)

[FIGURE 2-16: Identifying a DMZ.](#)

[FIGURE 2-17: Windows Firewall with Advanced Security.](#)

[FIGURE 2-18: Configuring password complexity in Windows.](#)

## **Book 9 Chapter 3**

[FIGURE 3-1: Configuring macros security settings in Microsoft Office.](#)

[FIGURE 3-2: Looking at virus protection software.](#)

[FIGURE 3-3: Enable real-time protection within antivirus software.](#)

[FIGURE 3-4: Updating virus definitions within antivirus software.](#)

[FIGURE 3-5: Remove spyware with Windows Defender.](#)

[FIGURE 3-6: MBSA identifies any security issues with your system.](#)

[FIGURE 3-7: Use LANGuard to identify security issues with a system.](#)

# Introduction

---

The CompTIA A+ Certified Professional certification is a well-recognized certification, and having this certification will serve as a basic foundation for a number of other certifications that you might pursue. The A+ exams test your knowledge of hardware and software used in today's computer world, and the certification is one of the most popular certifications that IT professionals attain to prove their hardware and software knowledge.

## *About This Book*

*CompTIA A+ Certification All-in-One For Dummies*, 5th Edition is designed to be a hands-on, practical guide to help you pass the A+ certification exams. This book is written in a way that helps you understand complex technical content and prepares you to apply that knowledge to real-world scenarios.

I understand the value of a book that covers the points needed to pass the A+ exams, but I also understand the value of ensuring that the information helps you perform IT-related tasks when you are on the job. That is what this book offers you — key points to pass the exams combined with practical information to help you in the real world, which means that this book can be used in more than one way:

- » **As an exam preparation tool:** Because my goal is to help you pass the A+ exams, this book is packed with exam-specific information. You should understand everything that is in this book before taking the A+ exams, but to help identify key points that you *must* know, look for icons called *For the Exam* to help you prepare.
- » **As a reference:** Rely on my extensive experience in the IT industry not only to study for (and pass) the A+ exams but also to help you perform common computer-related tasks on the job. I hope you find this book a useful tool that you can refer to time and time again in your career.

# *Conventions Used in This Book*

Each chapter in this book has different elements that help you prepare to pass the A+ exams. Each chapter holds the following features:

- » **Icons:** Look for the icons used in each chapter to draw your attention to information needed for the A+ exams or in the real world. For more details on the icons I use, check out the later section, “[Icons Used in This Book](#).”
- » **Getting an A+:** Found at the end of each chapter, the “Getting an A+” summary covers key points you should remember for the exams.
- » **Prep Test:** Following each chapter’s “Getting an A+” section, you can find example questions to help review the chapter content and prepare you for the A+ exams. Be sure to do the review questions with each chapter! Then, after you complete the book, check out the practice exams that accompany this book on the [www.dummies.com](http://www.dummies.com) website. These practice exams designed to function like the real exams, with the same level of difficulty. (See the section, “[Online test bank](#),” later in this Introduction for more information about how to access these practice exams.)

## *Foolish Assumptions*

I make a few assumptions about you as a reader and have written this book with these assumptions in mind:

- » **You are interested in obtaining the A+ Certification.** After all, the focus of this book is helping you pass the exams.
- » **You have a computer to work on.** To perform the labs found on the companion website, you need a computer that you can take apart and install a copy of Windows on. I recommend using virtualization software such as Hyper-V or Virtual Box to create a few different virtual machines and perform installation and configuration tasks of the different operating systems.

**» You will study hard and do as much hands-on work as possible.**

There is a lot of content covered in the A+ exams, and you will most likely need to read over the information a few times to ensure that you understand everything. You should also experiment as much as possible after you read a particular topic. For example, after you read about how to add a hard drive on a computer, you should get a second hard drive and add it to your computer. Or if you are reading about Windows utilities, try each one to be sure you are comfortable with what the utility looks like and what it can do.

# *How This Book Is Organized*

Like all *All-in-One For Dummies* books, chapters are organized into minibooks. The chapters in each minibook are related by a specific theme or topic. For example, [Book 9](#) — “Securing Systems” — contains all security-related content needed to pass the A+ exams.

## *Pre-Assessment*

Before you dive into the minibooks, you’ll find a set of pre-assessment questions to test your initial knowledge of the areas covered by the A+ exams. Take time to review each question to see where you stand, and then verify your work with the answers that follow. Use the chapter reference given to learn more about the topic related to the question.

## *Book 1: Setting the A+ Groundwork*

In this minibook, you discover what A+ Certification is all about and what you will be tested on when taking the A+ exams. You also find out some basic safety guidelines and general “soft skills,” such as how to communicate with customers.

## *Book 2: Inside the Box*

In [Book 2](#), you find out about the inside of a computer and what makes it tick. You venture into the innards of your computer, such as motherboards, memory, and processors, and also see how to install and upgrade these components.

## *Book 3: Outside the Box*

[Book 3](#) discusses topics related to what goes on outside the computer. You find out about the different ports on the back of the computer and how to install devices, such as video cards, sound cards, and network cards that give you output (think sound and video).

## *Book 4: Maintenance and Troubleshooting*

The maintenance and troubleshooting minibook discusses how you care for the computer to prevent problems or hardware failure. This minibook

also discusses how to troubleshoot different hardware components and how to diagnose the problem.

## ***Book 5: Operating System Basics***

Book 5 is a special minibook because it makes the transition from hardware topics to operating system topics. In this minibook, you find out the purpose of an operating system and which major files an OS needs in order to run. You also discover how to install and upgrade Windows.

## ***Book 6: Managing the Operating System***

In this minibook, I discuss and demonstrate in a hands-on way how to manage aspects of the Windows operating systems. You find out how to load drivers and how to install and support applications and start using a number of troubleshooting tools available within Windows.

## ***Book 7: Recovering Systems***

In this minibook, you discover which core files are needed to start up a Windows computer and how to fix computers that fail to boot up. You also find topics related to system recovery, such as how to back up the system and perform a restore operation.

## ***Book 8: Networking***

The A+ exams test your knowledge of basic networking concepts and ensure that you know how to network two computers. This minibook gives you the networking background you need to pass the A+ exams. You discover the basics of networking technologies and figure out how to troubleshoot systems on a TCP/IP network.

## ***Book 9: Securing Systems***

This final minibook covers topics related to securing your environment. In this minibook, I cover fundamental terms related to network security and also how to perform such tasks as creating user accounts, setting permissions, performing virus scans, and updating Windows.

## ***Appendix***

The Appendix includes an exam objective mapping table that lets you know where in the book each of the exam objectives are covered. This is very useful when you are preparing for the A+ exams to make sure you know each point in the objectives.

## *Icons Used in This Book*

I use a number of icons in this book to draw your attention to pieces of useful information.



**FOR THE  
EXAM**

This icon gives you a heads-up on information you should absolutely know for the A+ certification exams.



**TIP**

Information that would be helpful to you in the real world is indicated with a Tip icon. Expect to find shortcuts and timesavers here.



**REMEMBER**

This icon is used to flag information that may be useful to remember on the job.



**WARNING**

Information that could cause problems to you or to the computer is indicated with a Warning icon. If you see a Warning icon, make sure you read it. The computer you save may be your own.





TECHNICAL  
STUFF

Detailed information that is not needed for the A+ exams or that is a step above the knowledge you absolutely need to know for the exams is indicated with a Technical Stuff icon.



ON THE  
WEB

This icon lets you know when you can find accompanying information or supporting documents on the companion website for this book at [www.dummies.com/go/aplusaio](http://www.dummies.com/go/aplusaio). For example, there are a number of lab exercises written for the book — when a topic has a related lab, it is indicated with this icon. See the following section, “[Beyond the Book](#)” for more information about the companion website.

## *Beyond the Book*

In addition to what you’re reading right now, this book comes with several additional online components that you can use to enhance your knowledge.

### *Companion website*

The companion website for this book is located at [www.dummies.com/go/aplusaio](http://www.dummies.com/go/aplusaio). Here you will find the lab exercises for the chapters. Labs offer the opportunity to get your hands dirty with a particular topic with real-world experience performing specific tasks.

### *Online test bank*

Comprehensive, realistic practice exams are available for free online to help you test your knowledge of the A+ Certification objectives. To gain access to the online practice exams, all you have to do is register. Just follow these simple steps:

1. **Register your book or ebook at Dummies.com to get your PIN. Go to [www.dummies.com/go/getaccess](http://www.dummies.com/go/getaccess).**
2. **Select your product from the drop-down list on that page.**
3. **Follow the prompts to validate your product, and then check your email for a confirmation message that includes your PIN and instructions for logging in.**

If you do not receive this email within two hours, please check your spam folder before contacting us through our Technical Support website at <http://support.wiley.com> or by phone at 877-762-2974.

Now you're ready to go! You can come back to the practice material as often as you want — simply log on with the username and password you created during your initial login. No need to enter the access code a second time.

Your registration is good for one year from the day you activate your PIN.

## ***Cheat Sheet***

A free access-anywhere Cheat Sheet that gives you pointers on some of the major Windows concepts such as boot files, recovery tools, RAID types, and troubleshooting utilities. You will also find information on hardware specs for bus architectures, USB, FireWire, and POST messages. To get this Cheat Sheet, simply go to [www.dummies.com](http://www.dummies.com) and search for “A+ Certification All-in-One For Dummies” in the Search box.

## ***Where to Go from Here***

The CompTIA A+ Certification is the most popular certification for individuals new to the IT industry and the certification world. After you pass the A+ exams, you might want to continue your certification path by studying for the following certifications from CompTIA:

- » **Network+:** A vendor-neutral certification that ensures the candidate understands networking technologies.

» **Security+:** After passing the Network+ certification, you may want to continue on the network topic with a certification that proves your network security knowledge.

# Pre-Assessment

---

The following questions are designed to areas of the CompTIA A+ Certified Professional exams that you may need to focus on when reading through this book. Take time to review each question and come up with the best answer for each question. Be sure to verify your work with the pre-assessment answers that follow, and use the chapter reference given to learn more about the topic related to the question.

## *Questions*

- 1. Which of the following drive types can benefit from periodic disk defragmentation?**
  - (A) HDD
  - (B) DVD-RW
  - (C) CompactFlash
  - (D) SSD
  
- 2. You are assisting a customer in an upgrade from Windows 7 to Windows 8.1. Which upgrade method would you recommend if the user states that the computer has been infected by malware in the near past?**
  - (A) Unattended installation
  - (B) Clean install
  - (C) Repair installation
  - (D) System reset
  
- 3. The appearance of a proprietary crash screen is likely an indicator of:**
  - (A) Improperly disconnected USB drive
  - (B) Corrupted Windows Update

- (C) Hardware incompatibility
- (D) Missing GRUB loader

**4. Which of the following Windows 8.1 features restores the entire system to its state at a previous point in time?**

- (A) Windows RE
- (B) System Restore
- (C) System Refresh
- (D) System Image Recovery

**5. Which of the following devices should you use if you need to share one keyboard and mouse with multiple computers?**

- (A) KVM
- (B) Port replicator
- (C) Set-top box
- (D) Riser card

**6. You plan to secure a network printer for a customer by implementing the WPA2 encryption protocol. Which connectivity method for the printer should you use?**

- (A) Bluetooth
- (B) 802.11
- (C) Infrared
- (D) USB 3.0

**7. You are helping a customer who needs a second wired Ethernet interface on her laptop computer. Which of the following is the recommended option?**

- (A) Install a PCI Ethernet card
- (B) Use a USB to RJ-11 dongle
- (C) Use a USB-to-RJ-45 dongle

(D) Disable the on-board WiFi adapter

**8. Which of the following file systems is common on Linux systems?**

- (A) HFS
- (B) FAT32
- (C) NTFS
- (D) EXT3

**9. A customer has dropped off a system to have the processor upgraded. Which of the following features of CPU sockets make replacement of the CPU easier?**

- (A) XD-bit
- (B) Virtualization
- (C) Cores
- (D) ZIF

**10. You are a service technician for an accounting firm and need to upgrade the RAM on a high-end desktop workstation. You grab an 8GB SODIMM module from inventory and are having trouble installing it. Which of the following represents the reason for the installation problem?**

- (A) The workstation only takes 4GB modules
- (B) The module is not compatible
- (C) High-end workstations use flash memory
- (D) High-end workstations use solid state memory

**11. You are installing a new motherboard for a workstation within your office. When connecting the power to the motherboard, you notice a 6-pin power connector. What component does this typically supply power to?**

- (A) Graphics card
- (B) CPU

- (C) SATA drives
- (D) EIDE drives

**12. You are configuring the security for a customer's wireless network. Which of the following identifies the least secure wireless encryption protocol?**

- (A) WPA
- (B) WPA2
- (C) WEP
- (D) TKIP

**13. You are configuring a small LAN for one of your customers. You would like to implement NAT. Which of the following devices would you use?**

- (A) Hub
- (B) Switch
- (C) Modem
- (D) Router

**14. You are configuring the security on a folder that resides on an NTFS volume and has been shared as Data. The NTFS permissions give Bob the modify permission to the folder, but the folder has been shared giving Bob the read permission. What are Bob's effective permissions when he connects to the shared folder?**

- (A) Full control
- (B) Read
- (C) Modify
- (D) No permission

**15. You have installed virtualization software on the computer and are trying to create a virtual machine but you continue to receive an error. What is most likely the cause?**

- (A) Disable cache memory in the BIOS
- (B) Enable XD-bit in the BIOS
- (C) Change the boot order in the BIOS
- (D) Enable virtualization in the BIOS

**16. You have been noticing that your server has been performing slowly over the last few days and now all of a sudden no one can make a connection to the server. Looking at server log files you have determined that the server was under attack. What type of attack likely occurred?**

- (A) DoS
- (B) MTM
- (C) Dumpster dive
- (D) Dictionary

**17. You are troubleshooting Bob's workstations to determine why he cannot get access to the Internet. You use the ipconfig command and get the following output. What is likely the cause?**

```
PS C:\> ipconfig /all
Ethernet adapter Ethernet:
Connection-specific DNS Suffix . : dcatt.ca
Description . . . . . : Qualcomm Atheros PCI-E Fast Ethernet
Physical Address. . . . . : 20-1A-06-34-2B-66
DHCP Enabled... . . . . : No
IPv4 Address... . . . . : 192.168.1.138
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.2.1
DNS Servers . . . . . : 192.168.1.1
```

- (A) There is no MAC address assigned to the system
- (B) The DNS suffix is incorrect
- (C) The default gateway address is incorrect
- (D) The DNS server is incorrect



- 18. CompTIA has a six-step problem resolution process. What is the third step in the process?**
- (A) Identify the problem
  - (B) Test the theory to determine cause
  - (C) Establish a plan of action to resolve the problem and implement the solution
  - (D) Document findings, actions, and outcomes
- 19. You are working with a computer that is having a problem loading the user profile and the Windows Explorer interface. You have access to the command prompt window. What command will terminate the runaway process named `RunAway.exe` with a PID of 3375?**
- (A) `Tasklist /FI RunAway.exe`
  - (B) `Taskkill /FI RunAway`
  - (C) `Tasklist /PID 3375`
  - (D) `Taskkill /PID 3375`
- 20. You are planning to move from your old office due to issues with power in the neighborhood. Within the neighborhood you are constantly being exposed to blackout, brownout, spikes, and voltage drops. Which device will protect you from all of these issues?**
- (A) Surge suppressor
  - (B) UPS
  - (C) Line conditioner
  - (D) Power tester
- 21. You have been called to a customer's computer to help her deal with a recent problem she has developed when starting an application. You think it may be due to components that are loading automatically when Windows boots and loads. Which tool can you use to disable services or perform a selective startup of Windows?**

- (A) `diskpart.exe`
- (B) `chkdsk.exe`
- (C) `msconfig.exe`
- (D) `defrag.exe`

**22. While managing a group of workers servicing computers in your repair shop, you have received complaints from them that they are seeing a lot of incidents of static discharge. They are worried about the components that they are working with. What steps can you take to reduce the chance of static discharge or ESD?**

- (A) Increase the relative humidity
- (B) Decrease the relative humidity
- (C) Increase the temperature
- (D) Decrease the temperature

**23. A user has called you while you are working on the support desk. He has an issue with power management settings that are being pushed out to users via Active Directory Group Policy Objects (GPO). After adjusting the GPO to correct the issue, you would like to have the client computer process the GPO changes immediately. What tool will you use to process the GPO changes?**

- (A) `attrib`
- (B) `gpresult`
- (C) `expand`
- (D) `gpupdate`

**24. You are working with a member of your IT administration team to set permissions on a Linux server on your network. You need to change the permissions granted to a group of users who will be accessing a directory. What command will you be using to change the permissions?**

- (A) `chmod`

- (B) `chown`
- (C) `grep`
- (D) `iwconfig`

**25. Your local IT administrator has made changes to `C:\boot.ini` to change the loading process for his Windows 8.1 computer, but this does not seem to have had any effect on the boot process. What component controls the boot configuration and thereby the boot process on a Windows 8.1 computer?**

- (A) `ntoskrnl.exe`
- (B) `winload.exe`
- (C) `ntdetect.com`
- (D) BCD

## Answers

1. **A.** The magnetic hard disk drive (HDD) definitely benefits from periodic disk defragmentation because its mechanical operation lends itself to fragmentation. *See Book 2, [Chapter 5](#).*
2. **B.** Personally, I wouldn't take a chance on an upgrade if the system is suspect. Instead, I recommend backing up the user state, performing a clean Windows 8.1 installation, and restoring the user state (which doesn't include program files) to the upgraded system. *See Book 5, [Chapter 3](#).*
3. **C.** Normally, the appearance of the “Blue Screen of Death” in Windows or the “Spinning Beach Ball of Death” (OS X) signifies a hardware incompatibility. For instance, you may have inadvertently installed the wrong RAM type in the system. *See Book 7, [Chapter 2](#).*
4. **D.** System Image Recovery involves creating an image of the entire system drive. Therefore, restoring a computer with a previously created recovery image restores the entire operating system

environment to its state at the previous point in time. *See Book 7, [Chapter 3](#).*

5. **A.** A keyboard-video-mouse (KVM) switch is exactly what you need in this situation. You'll often find KVMs in data centers so that engineers can easily manage several systems located in the same server rack. *See Book 3, [Chapter 2](#).*
6. **B.** WiFi Protected Access 2 (WPA2) encryption is available on IEEE 802.11 WiFi networks only. While we're on the subject, be sure never to use Wired Equivalent Privacy (WEP), which is a fundamentally broken WiFi security protocol. *See Book 3, [Chapter 4](#).*
7. **C.** If you remember that Ethernet uses the RJ-45 connector type, then you'll answer this question correctly every time. Recall that RJ-11 is used for traditional telephones and (yuck) analog modem connections. *See Book 3, [Chapter 6](#).*
8. **D.** Linux computers typically use the EXT3 or EXT4 file systems, although they can support other file systems for compatibility with other operating system platforms. *See Book 5, [Chapter 3](#).*
9. **D.** A zero insertion force (ZIF) socket is a type of socket used with PGA and LGA chips to allow easy removal and installation of the processor chip. A ZIF socket has a lever that allows releases the processor and allows it to be lifted out of the socket. *See Book 2, [Chapter 2](#).*
10. **B.** Desktop computers use DIMM when installing RAM into the computer. SODIMM are used by laptop computers. *See Book 2, [Chapter 3](#).*
11. **A.** The 6-pin power connector is typically used to supply power to the PCIe graphics card. *See Book 2, [Chapter 1](#).*
12. **C.** In today's day and age, you should avoid the WEP encryption protocol when configuring wireless security because the encryption with WEP is easy to crack. When encrypting wireless traffic, always use the newer protocols such as WPA2. *See Book 8, [Chapter 2](#).*
13. **D.** Network address translation, or NAT, is a network service that allows multiple systems and devices on the network to access the

Internet using a single IP address. NAT is typically a service provided with routers. *See Book 8, [Chapter 1](#).*

14. **B.** When NTFS permissions conflict with shared folder permissions, the most restrictive permission will be the effective permission. In this case, read is more restrictive than modify. *See Book 8, [Chapter 3](#).*
15. **D.** Before trying to configure virtual machines on the system, you should verify that virtualization support has been enable within the BIOS. *See Book 2, [Chapter 4](#).*
16. **A.** A denial of service attack (DoS) is when a system is overloaded with requests from a hacker, which causes the server to be unresponsive to valid requests from clients, or eventually crashes the server. *See Book 9, [Chapter 1](#).*
17. **C.** The default gateway address is incorrect. The default gateway address must reference the same network ID as your client system; in this case, the address should start with the network ID of 192.168.1.x instead of 192.168.2.x. *See Book 8, [Chapter 3](#).*
18. **B.** The third step in the CompTIA problem is Test the theory to determine cause. *You can review all six steps in Book 1, [Chapter 2](#).*
19. **D.** `taskkill.exe` supports several options to terminate a task either by name or by PID. To terminate a task by PID, you would use `taskkill.exe /PID 3375` and to terminate by name, you would use `taskkill.exe /IM notepad.exe`. Read through *Book 6, [Chapter 3](#)*.
20. **B.** The only device which protects against a blackout is a UPS. *See Book 2, [Chapter 6](#).*
21. **C.** The System Configuration Utility (`msconfig.exe`) can be used to perform a selective startup of Windows to assist in troubleshooting issues. `Defrag.exe` is used to defragment the disk; `diskpart.exe` is used to partition a disk; and `chkdisk.exe` is used to check your disks for errors. *See Book 6, [Chapter 4](#).*
22. **A.** To reduce the chance of ESD, you should increase the relative humidity. ESD risks are increased in dry air. *Locate this information in Book 4, [Chapter 1](#).*

23. **D.** The command `gpupdate` is used to trigger the processing of Activity Directory GPOs, while `gpresult` will display the effective results of GPOs. The command `attrib` is used to adjust file attributes, such as read-only and archive, while `expand` is used to expand compressed system files. *See Book 5, [Chapter 5](#).*
24. **A.** The command to change permissions is `chmod`, while `chown` will change the owner and group who has access to the resource. The `grep` command will display and filter contents of files or output from commands, and `iwconfig` is used to manage wireless configurations. *Review Book 5, [Chapter 1](#).*
25. **D.** The BCD or Boot Configuration Database stores boot configuration settings which are used during the boot process. The file `ntoskrnl.exe` is the operating system kernel; `winload.exe` is the operating system loader; and `ntdetect.com` was an OS load file from older Windows OSes. *Review Book 5, [Chapter 6](#).*

# Book 1

## Setting the A+ Groundwork

### Contents at a Glance

#### Chapter 1: The 2019 A+ Exams

[CompTIA A+ Certification and Why You Need It](#)

[Checking Out the Exams and Their Objectives](#)

[Using This Book to Prepare for the Exams](#)

[Making Arrangements to Take the Exams](#)

[The Day the Earth Stood Still: Exam Day](#)

#### Chapter 2: A+ Best Practices

[Using Troubleshooting Procedures and Good Practices](#)

[Implementing Change Management](#)

[Professionalism and Communication](#)

[Getting an A+](#)

[Prep Test](#)

[Answers](#)

#### Chapter 3: Protecting Yourself and Your PC

[Gathering Tools of the Trade](#)

[Avoiding the Dreaded ESD](#)

[Watching Out for EMI](#)

[Safety First!](#)

[Handling Toxic Waste](#)

[Environmental Impacts and Appropriate Controls](#)

[Exploring Ergonomics](#)

[Getting an A+](#)

[Prep Test](#)

[Answers](#)

#### Chapter 4: An Overview of System Components

[What Is a Computer?](#)

[Looking Inside the Box](#)

[Checking Outside the Box](#)

[Getting an A+](#)

[Prep Test](#)

[Answers](#)



# Chapter 1

## The 2019 A+ Exams

---

### IN THIS CHAPTER

- » Understanding A+ Certification and its benefits
  - » Looking at the exams and their objectives
  - » Preparing for the exams
  - » Arranging to take the exams
  - » Test day
- 

So, you are interested in taking the CompTIA A+ certification exams? This chapter introduces you to the exams and gives you a good idea of what you can expect when you go to take them. Knowing what to expect in regard to the exam procedures and format will remove that uncertainty, which can weigh on your mind. Read through the procedures here; then you will be able to focus on the exam facts, which will help you breeze through the exams.

I hope that this chapter helps remove some of that normal fear of the unknown by giving you information about the actual test-taking process. This chapter will also help you develop good test-taking skills.

## *CompTIA A+ Certification and Why You Need It*

The benefit of the CompTIA A+ Certification is that it is proof that you know and have validated the hardware and software knowledge necessary to troubleshoot and repair computers. The CompTIA A+ Certification can be presented to employers and clients alike as proof of your competency and skill in this area. This certification is valid for three years from the

day that you attain the certification, after which time you must renew by taking the newest version of the exam, or by taking a higher level certification exam. You can find out more on the subject at

<https://certification.comptia.org/continuing-education>.

Formed in 1982, CompTIA was originally named the Association of Better Computer Dealers. It is a company focused on providing research, networking, and partnering opportunities to its 19,000 members in 100 countries. In 1993, in response to the need for vendor-neutral, entry-level PC certification, the company created the A+ Certification.

Prior to CompTIA creating the A+ Certification, there were many places where a person could get hardware and software certifications. However, such training was often very expensive, difficult to get, and not designed for accessibility for most people. Microsoft, Novell, IBM, and other software companies offered software certifications, but these were specifically focused on teaching high-level support skills for these products, were difficult for average users or support people to attain, and lacked relevance for most day-to-day work.

IBM, HP, Compaq, Sun, and other hardware companies offered hardware repair and maintenance certifications, but again, these were specifically focused on their hardware — and more on the peculiarities of their own platforms, and not always covering the basics of configuration and maintenance. CompTIA stepped in to fill the gap that a majority of users fell into, which is a hardware and software neutral certification that covered all the basics required by a support person. This certification can then be followed by vendor-based certifications, if desired, but the A+ Certification by itself proves a firm grasp of the basics.

An A+ Certification gives employers confidence that existing employees or new recruits have a level of knowledge with which they can do their jobs efficiently. It also gives employers a yardstick against which recruits and employees can be measured. And an A+ Certification also allows clients to rest assured that the person they hire to fix their computers has the knowledge to do so without blowing up equipment or deleting valuable data. This provides clients with peace of mind and increases

repeat business. In the end, with the CompTIA A+ Certification on your side, you have more opportunities open to you in your career path.

## *Checking Out the Exams and Their Objectives*

You have to take two exams to get your CompTIA A+ Certification. Both exams are required. The first required exam is the CompTIA A+ Exam 220-1101, which focuses on the hardware aspects of computer repair. The second required exam is the CompTIA A+ Exam 220-1102, which focuses on configuring and troubleshooting the software aspects of a system in a corporate network environment.

Revised exams for CompTIA A+ were released in 2019. In addition to traditional multiple-choice questions, the CompTIA A+ exams include an unspecified number of performance-based questions (PBQs); these are short exercises that test your ability to solve problems in a simulated environment. The CompTIA website has a sample performance-based question that can be viewed at

<http://certification.comptia.org/testing/about-testing/performance-based-questions-explained>.

You have 90 minutes to complete each exam; [Table 1-1](#) contains the number of questions and passing score for each exam. CompTIA is releasing the exams as linear format exams — standard timed exams — taken on a computer. After CompTIA gathers grading statistics, it might re-release the exams as adaptive exams (what CompTIA has done in the past), but there is no current announcement that this is planned. In this adaptive exam, you will be asked a minimal number of questions (usually about 15), and then asked additional questions based on any incorrect answers. The exam adapts to your wrong answers by choosing additional questions for you from the area where you are weaker.

**TABLE 1-1 A+ Exam Information**

<i>Exam</i>	<i>Number of Questions (Maximum)</i>	<i>Minimum Passing Score</i>
-------------	--------------------------------------	------------------------------

<i>Exam</i>	<i>Number of Questions (Maximum)</i>	<i>Minimum Passing Score</i>
A+ Exam (220-1001)	90	675
A+ Exam (220-1002)	90	700

## *The CompTIA A+ Exam 220-1001*

The CompTIA A+ Exam 220-1001 covers the basics of computer hardware, network hardware, and mobile devices topics. [Table 1-2](#) provides a breakdown of the exam areas that are covered on the CompTIA A+ Exam 220-1001. This exam puts heavy emphasis on computer components and hardware.

**TABLE 1-2 CompTIA A+ Exam (220-1001)**

<i>Domain</i>	<i>Percentage of Examination</i>
1.0 Mobile Devices	14%
2.0 Networking	20%
3.0 Hardware	27%
4.0 Virtualization and Cloud Computing	12%
5.0 Hardware & Network Troubleshooting	27%
Total	100%

## *The CompTIA A+ Exam 220-1002*

In addition to the CompTIA A+ Exam 220-1001, you have to take a second exam. This exam is the CompTIA A+ Exam 220-1002, which is designed to measure skills required to maintain and troubleshoot operating systems and mobile devices. The breakdown of the exam components is covered in [Table 1-3](#). Based on the domain breakdown, this exam has the widest breadth of topics for a well-rounded IT professional.

**TABLE 1-3 CompTIA A+ Exam (220-1002)**

<i>Domain</i>	<i>Percentage of Examination</i>
---------------	----------------------------------

<b><i>Domain</i></b>	<b><i>Percentage of Examination</i></b>
1.0 Operating Systems	27%
2.0 Security	24%
3.0 Software Troubleshooting	26%
4.0 Operational Procedures	23%
Total	100%

# *Using This Book to Prepare for the Exams*

Exams are stressful events for most people, but if you are well prepared, your stress level should be much lower. If you read and understand the material in this book, you should have no problem with any of the exams. The review questions at the end of each chapter in this book, and the sample exams on the book's companion website at [www.dummies.com/go/aplusaio](http://www.dummies.com/go/aplusaio) are all designed to prepare you for what lies ahead. This book takes a holistic approach to studying for the exams. Review all the material found here, and then you will be prepared to go and take either of your exams you choose because they can be taken in either order. I recommend taking both of your exams in a short time frame to avoid forgetting the information you have learned.



**TIP**

Examine the objectives for each chapter before diving into the content so that you can use them as a guide to which sections you might need to focus on. After thoroughly reading the content of the chapter, attempt the Prep Test section at the end of the chapter. If you do poorly on the Prep Test, go back to the objectives to see where you need more effort. When you re-read the chapter sections, try to examine the content from another viewpoint to help you associate the information with the questions and the objectives. For example, a differing viewpoint might be that of a computer user, a help desk employee, or a desktop support technician. After you can complete the Prep Test in each chapter with an 85 percent or better score, move on to attempt the practice exams on the companion website. If you are unable to achieve a mark of 85 percent or better, you should continue to review the areas in which you are weak.

# *Making Arrangements to Take the Exams*

The A+ certification exams can be scheduled at Pearson VUE testing centers. For more information about scheduling your exam, check the CompTIA A+ Certification page on CompTIA's website at

<http://certification.comptia.org/certifications/a>

The cost to take the A+ exams is \$219 (US) per exam. CompTIA Premier members receive a discount.

## *The Day the Earth Stood Still: Exam Day*

Knowing what to expect on the day of the exam can take some of the pressure off of you. The following sections look at the testing process.

### *Arriving at the exam location*

Get to the exam location early on the day of the exam. You should arrive at the testing center 15 to 30 minutes before the exam starts. This keeps you from being rushed and gives you some temporal elbow room in case there are any delays. It is also not so long that you will have time to sit and stew about the exam. Get there, get into a relaxed frame of mind, and get into the exam.

To check in for your exam, you will need two pieces of identification: One must be a government-issued photo ID, while the other must have your name and signature. This may vary in some regions of the world.

When you get to the test site, before you sign in, take a few minutes to get accustomed to the testing center. Get a drink of water. Use the restroom if you need to. The test will be 90 minutes, so you should be able to last that long before another break.

Now relax. Getting to the exam site early gives you this privilege. You didn't show up early just to stew and make yourself more nervous.

If you feel prepared and are ready to go, you might want to see whether you can start the test early. As long as a testing seat is available, this is usually not a problem.

You will not be able to take anything into the testing room. You will not be allowed electronics, paper, and so on. The testing center will provide you with something to write with and to write on, which they will take back at the end of test.

## *Taking the exam*

In the testing room, and depending on the size of the testing center, there may be as many as eight computers set up. Each computer represents a testing seat.



**TIP**

Because the exam consists of multiple-choice questions and an unspecified number of performance-based questions, take it slow — or at least pace yourself. Trying to complete the questions too quickly will no doubt lead you to errors. When you are about to start the exam, you will see onscreen how many questions there will be, and how long you have to complete the exam. Be sure to read the onscreen exam instructions at the start of the exam; they do change from time to time.

Based on the number of questions and your exam time, figure out how long you can spend on each question. On average, you have slightly more than one minute per question. Take your time, but be aware of your time for the exam overall. Think of it this way: When you have completed 25 percent of the exam, you should have used only 25 percent of your allotted time.

Read the entire question and try to decide what the answer should be before looking at the answer choices. In most cases, you will find a few key words that are designed to remove any ambiguity in the question, as well as a few distracters and useless information designed to throw you



off. If you do not notice these key words, the question will seem vague. If this is the case, re-read the question and look for the key words. Exam questions are written by many authors, so the style of writing for each question could differ.



**REMEMBER** Don't overcomplicate the questions by reading too much into them. Besides the key words and the distracters, the question should be straightforward. In some cases, the question might ask for the best choice, and more than one answer might seem correct. Choose the one that is *best* — the quickest, most likely to succeed, least likely to cause other problems — whatever the question calls for. The best choice is always the right choice.

After identifying the key words and distracters, follow these additional steps:

**1. Eliminate choices that are obviously wrong.**

Most questions will ask you to choose one of four answers. Some questions will ask you to choose all that apply and have as many as eight choices. You should be able to immediately eliminate at least one choice — perhaps two. Now the odds of choosing the right answer have gotten substantially better. Re-read the question and the remaining choices carefully, and you should be able to locate the correct answer.

**2. If you don't have a clue which of the remaining choices is correct, mark an answer.**

On a standard timed exam, you can review your answers. Not answering a question is automatically wrong, so if you at least *have* an answer, it might be right. You might also find information on other questions in the exam that triggers the correct answers for questions you were not sure of.

**3. Make your choice and leave it.**

Unless you have information that proves your choice is wrong, your first instinct is usually correct.

CompTIA has not announced an adaptive exam at the time this was written, but if it adds the option, here are a few things to know about the adaptive exam process, as it varies from the standard form exam. The adaptive exam delivers a series of questions to you. If you answer a question incorrectly, you get additional questions in that category. You can't review or change your answers on the adaptive exams like you can with standard timed exams. Because skipped questions are automatically wrong and you do not have the ability to change them, you must provide an answer to the question before moving to the next question. You are allowed to attempt to answer a finite number of questions (known only by CompTIA) before the test "decides" that you really don't know what you need to know to pass the test. If you exceed the allowed number of wrong answers (again, known only by CompTIA), the exam ends; you fail. (But that won't happen to you because you bought this wonderful book!) Currently the A+ certification exams are not adaptive.

If you get all the initial category questions correct, you can pass the exam in relatively few questions. If you get an initial category question wrong in a category in which you are weak, though, you will find the adaptive format very difficult. You won't know exactly how many questions you have to answer to complete the exam, so the end of an adaptive exam will always come as a surprise — hopefully, a good one.

If you are taking the nonadaptive exam, you are allowed to mark questions and come back to them later. However, I recommend selecting an answer for every question, even if you are unsure about it, because you might run out of time before you can review previous questions.



**REMEMBER** Your first choice is usually correct — don't second-guess your first choice! Change your answer only if you're absolutely positive it should be changed.

Regardless of which type of exam CompTIA has available for you when you take your exam (adaptive or standard timed), you are given a Pass/Fail mark right on the spot after completing the exam. In addition, you get a report listing how well you did in each domain. If you don't pass (or even if you do), you can use this report to review the material on which you are still weak.

### ***How does CompTIA set the pass level?***

CompTIA uses a scale score to determine the total number of points that each question on the exam will be calculated from. Your final score will be between 100 and 900. In any case, the passing score (not a percentage, due to the scale) varies from one exam to the others. The scale score system allows the number of points assigned to questions to vary between each copy of the exam, which makes it harder for test candidates to compare scores across exams. You can find more information about the exam at

<https://certification.comptia.org/certifications/a#examdetails>.

CompTIA has a retake policy. If you do not pass on the first attempt, you can take the exam again. There is no waiting period to make your second attempt at the exam, but you have to wait at least 14 calendar days before your third or subsequent attempts. The CompTIA exam retake policy can be found at <https://certification.comptia.org/testing/test-policies/comptia-certification-retake-policy>.

# Chapter 2

## A+ Best Practices

---

### IN THIS CHAPTER

- » Knowing your troubleshooting techniques
  - » Working within the boundaries of a change management system
  - » Communicating effectively and professionally
- 

As a CompTIA A+ Certified Professional, you will often need to troubleshoot systems as well as deal with customers or clients. For you to complete these tasks, you need good troubleshooting skills, and you also need to develop good customer-relation skills.

This chapter examines the basics of troubleshooting. These basics are not centered on specific hardware components, but rather on basic methodology that is used to solve problems. This methodology will not change even though the underlying technology might change.

Troubleshooting specific components is covered in Book 4, [Chapter 2](#).

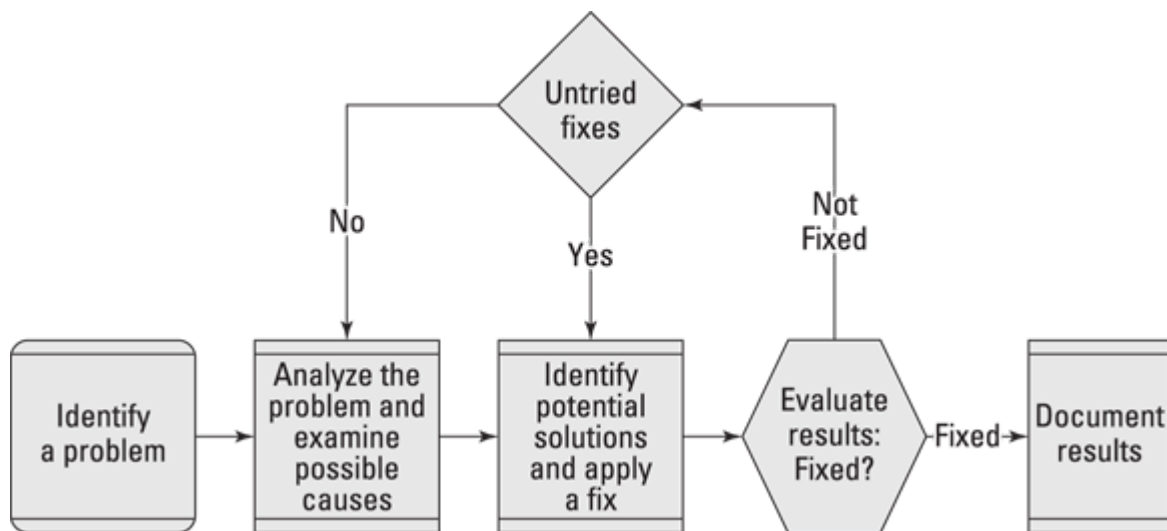
When solving problems for customers — internal or external customers — you will likely need to talk to them. This chapter takes a look at the communication skills that help you maintain a high level of professionalism.

## *Using Troubleshooting Procedures and Good Practices*

Many people say that troubleshooting skills cannot be learned, but this is not true. If you are methodical or just curious, you will probably have an easier time troubleshooting. However, anyone can learn the practical order to follow when troubleshooting problems. Follow the steps in this

chapter, and you should have an easy time when it comes to troubleshooting.

The two main sections of troubleshooting are *hypothesis generation* and *hypothesis evaluation*. In other words, based on the symptoms that you see, you create a list of things that might be wrong and then test to see whether any of them are actually the problem. [Figure 2-1](#) shows a rough outline of general troubleshooting procedures.



**FIGURE 2-1:** Basic troubleshooting steps.



**FOR THE  
EXAM**

CompTIA lays out its recommended troubleshooting process as follows, but remember to take any corporate policies into account when going through the process:

1. Identify the problem.
2. Establish a theory of probable cause.
3. Test the theory to determine cause.
4. Establish a plan of action to resolve the problem and implement the solution.

5. Verify full system functionality and if applicable implement preventive measures.
6. Document findings, actions, and outcomes.

To troubleshoot any system, you need to know how that system is supposed to function and what options can be changed or might fail. This information allows you to quickly assemble a list of hypotheses. Once you have a list of potential causes in hand, you can move on to figuring out potential solutions. In some instances, you might approach the problem starting at a general level and then work down to specific components.

Conversely, you might look at entire systems, like the power system, in a sequential manner. In most cases, your potential causes can be placed on an imaginary line that forms a resolution path. The resolution path forms a sequential chain of possible causes for the issue, starting at one point and moving to another. For instance, if a computer does not power up, you can start testing at the electrical socket; move to the power supply, power supply connectors, power switch, motherboard; and then move to the devices. This process moves through the sequential chain along the possible path that power would flow. Following a possible resolution path from one end to the other is sometimes referred to as the *layered* or *linear approach*.



**TIP**

The term *layered* is often used when discussing networking issues because the layers in the networking model are easily definable and are often referenced. For more information about the layered network model, see [Book 8](#), which discusses networking.

Most systems that make up computer systems and networks can be broken down into layered models, and troubleshooting can move through these layers. Another example of layered troubleshooting is a gasoline engine, with its two major systems: the electrical system and a fuel supply system. The electrical system has layered troubleshooting starting at a power source (say, a battery) through power supply cables, a distributor, and finally to a spark plug. The fuel supply system starts with fuel storage,

supply lines, a pump, and filter, and then ends at a combustion chamber. In the event of a problem, both systems can be reviewed and tested from end to end, in a linear or layered manner, until the problem is located.

## *Identify the problem*

When you are presented with a problem, the first step to identifying the problem is to question the system's user. This shouldn't be a police interrogation, nor should you accuse the user of causing the error. You might discover, after all is said and done, that the user actually *did* cause the error, but you should never assume that upfront, or you will quickly become an adversary instead of an advocate.

The information you gather from the user helps you set the scope of the problem. Many users start with the simple, "It's broken!" It is up to you to figure out how "it" is "broken," and you do that by asking simple questions: "What issues are you having with it? What is it not doing? Does it always happen or only at certain times?"

Even if the user gives you a better starting point, you will likely still need to ask some questions to refine the scope of the problem. Here are some things to keep in mind while you try to identify the problem:

- » **Identify changes to the computer or network.** Some errors are caused by the user or his surroundings. The user should always be asked up front, in much the same way a doctor asks whether his patient's lifestyle has changed or whether he is on any medication. Question the user whether he made any changes to the computer by installing software, changing hardware, or changing the computer's location. This often provides you with an early lead to the possible problem.
- » **Identify environmental or infrastructure changes.** When working with infrastructure components with a customer, the same holds true: Were there changes in the Active Directory Group Policy Objects, networking, servers, or even the building's power? If the customer is having issues with computers rebooting unexpectedly, the trouble could be traced back to recent electrical work.

- » **Review system and application logs.** The logs on a computer or device can provide great insight into changes on the device, provide an indicator to the source of this issue, as well provide you with an indication that the problem has been fixed. If you always see the same error in the log before the reported problem occurs, this may indicate the root cause of the reported problem, and resolving the source of that error may also resolve reported problem.
- » **Break big problems into smaller pieces.** Continuing with the doctor analogy (see the first bullet), the “I feel sick” statement causes a doctor to ask questions and build a list of symptoms. That list of symptoms (sore throat, headache, runny nose, gaping hole in abdomen) might be easier to deal with if broken down into groups of symptoms rather than being treated as a whole. The doctor might then treat each group of symptoms individually. The same applies to computer problems. That “broken” computer might be malfunctioning because of a variety of smaller problems: insufficient RAM, a fragmented hard drive, malware, Trojans, and poor networking protocol configuration. If the problems are broken down instead of being treated as a whole, you can approach each item separately.
- » **Prioritize problems and decide in which order they should be tackled.** With your list of problems, decide which are the most critical and should be approached first. For instance, if the hard drive is corrupted *and* you need to re-install or upgrade the operating system, fix the issue with the hard drive before performing the software upgrade.



**REMEMBER** In most cases, you prioritize the issues based on the impact to the user and the impact of other fixes implemented at a later time. One rule I live by is, “Fix the business problem first.” For example, if you are working for a stock trader, she needs her stock trading program working immediately, but she might be willing to wait for a fix to the word processing program.



## *Establish a theory of probable cause*

For each problem you work on, decide the scope of the problem. This can be done by testing. The initial tests you conduct determine the scope of the problem. Say you go to a doctor for an upset stomach. She asks stomach- and food-related questions and then probably runs some basic tests to determine whether the problem is an ulcer, an allergy, or just some bad sushi.

The same is true with computer issues. You ask questions and then perform rudimentary tests to determine the scope of the issue. For example, after being told that a printer does not print, you might verify that its cables are in place, it powers up, it has toner or ink, and it accepts commands from the computer. These rudimentary checks allow you to see how large the problem is; from there, you can perform additional analyses. For example, if the printer is passing paper but the pages come out blank, your list of potential causes can be reduced because it is not a power issue. Rather, the problem is either with the transfer of the printing material — the ink or toner — or with the interpretation of the commands from the computer. With this narrowed list of potential causes, you can move on with addressing the problem.

## *Don't forget to question the obvious*

When I get the messages, Missing Operating System, NTLDR is missing, BOOTMGR is missing, or messages related to winload.exe or BCD not being found, the first thing I do is look for a floppy disk or USB drive that was left plugged into the system. For power problems, is it plugged in? For network problems, is the cable plugged into the correct jack? These simple first steps are often overlooked by the user. Just because it is obvious to you does not mean it is obvious to the user. If the solution is not obvious, go back to your layered approach — it will not let you down.

## *Research to find potential fixes*

If you run out of ideas for a specific problem, do a little research. The “[Documentation resources](#)” sidebar later in this chapter gives you some ideas about where to begin.



**REMEMBER** There is nothing wrong with you, as a CompTIA A+ Certified Professional, not knowing the solution to a particular issue with a specific product. What is important is that you know where you can find the answers — quickly.

### ***Test the theory to determine cause***

Once you have a theory as to the possible cause of the issue, come up with a test to verify your theory. You will then be able to run your test to prove your theory true or false. If the theory proves to be true, you can plan to correct the issue. If the theory proves to be false, you will need to come up with a different theory or possible cause. For example, with a computer that is running slowly, you may notice that it has very little free memory, so increasing RAM may resolve the issue, but if it does not, then you may want to review CPU utilization, as the issue may be a process that is highly active, or perhaps consuming excessive RAM.

### ***Consider corporate policies, procedures, and impacts***

Before making any changes to the production environment, always consider any corporate policies, procedures, and impacts. Many customers I deal with have blackout periods for changes in the environment during critical times of the year, such as the month leading up to year end and the December holiday period. These periods either represent times of great risk if systems stop working, or times of reduced staffing, and are not times when any problems caused by a change will be welcome.

When working with a customer, I often ask if this is a change we can make without undertaking any change management procedures, such as a Change Management Board review. (You learn more about the proper change management practices later in this chapter.) If you feel that there is risk in changing a setting, then consider testing it out in a lab or ensure you follow the customer's change management process.

### ***Back up any settings or files you need to change***

You don't want to introduce more problems to a system than it had when you started. Before changing any basic input-output system (BIOS) or application settings, record the original settings — or back them up. For instance, if an application you are troubleshooting stores its configuration in a text or binary file, copy that file so you can quickly restore it to the initial state if your solution doesn't work.

Some computers allow you to make a backup copy of your BIOS settings, which are stored in complementary metal-oxide semiconductor (CMOS) memory; or back up the existing BIOS prior to overwriting it with an upgrade. Some things cannot easily be reversed, like the application of a Service Pack, so care should be taken when doing those tasks, such as setting a restore point or making a full system backup.



**REMEMBER** If you need to make a large number of changes, it is a good idea to take a complete backup of the computer prior to starting your troubleshooting process so that you will be able to retrieve any settings or files that are deleted or modified.

### *Test one configuration change at a time*

This step is required to know what the fix actually is. If you change five things and the problem component now works, you don't know which change made the difference. In some cases, you might incur monetary costs. For instance, if the computer starts to blue screen on boot and you suspect a hardware fault, you could change the disk controller, hard drive, RAM, CPU, and power supply. After that, if the problem no longer exists, what was the solution? Are you going to replace all five components the next time you have the issue? By substituting one item at a time and testing at each step to re-create the issue, you will know which change you implemented corrected the problem.

### *Prioritize potential fixes for the problem*

After you spent time researching the symptoms, now you have a long list of items to check and possible solutions to apply, and you must prioritize them. You can put the most-likely fix at the top of your list, or you can put

the quickest and least-disruptive fix at the beginning of the list. In most cases, you will likely do the latter.

For instance, a good fix for many software-related problems is to reimage the computer or re-install the application. Although this often fixes the problem, it can be time consuming for you and disruptive for the user. Re-installation often involves checking for local files that need to be backed up, backing them up, verifying application settings, restoring the computer operating system, restoring backed-up user files, and reapplying settings. This usually leaves a lot of settings that the user needs to reset when she runs the application(s) for the first time after re-installation. Because this is time consuming and disruptive, it should be left toward the end of the list of options. Rather, the list should begin with items such as verifying application settings, testing new-user profiles, and applying other quicker and less-disruptive fixes.

At each step of the analysis and application of potential fixes, evaluate the results. By evaluating often, you will know what is working, what is not, and what additional problem you might have caused. At any time, the results might cause you to change your initial hypothesis and choose to pursue a different path. Changing your hypothesis should be done only if there is sufficient proof that your initial statements were in error, or you might find yourself running in circles.

### *Test related components*

Sometimes, a symptom in one area is caused by a problem in another. The classic example with computers is being asked to look at a computer that is reported as slow, and has an extremely active hard drive. You can test the hard drive and related cables, use diagnostic utilities to test its health, swap it with another, only to not find a solution. Then you have to take a step back and evaluate other system components, such as memory. In many cases, a lack of RAM can cause excessive paging, which causes high disk activity, so the solution to the problem might be to add RAM to the computer and not do anything with the hard drive. If you did not look at the related component (RAM), you would not have been able to solve the problem with the active hard drive. In some cases, you might need to do some research to know what components of the system are related. Don't

just go for the obvious: Test related systems as well. That might be where the actual issue is.

### *Call in the “big guns” and escalation*



**REMEMBER** You are not alone in this exercise. In many cases, there may be internal resources to which you may escalate a problem that you cannot resolve. If there are no internal resources above you, then in many cases there is a vendor or manufacturer that you may be able to contact. Many vendor support departments have seen your problem and can offer steps to resolve the issue. Never be afraid to realize your limits and ask for help when you need it.

Once you have exhausted your knowledge of the product or issue, and once you have tested all your theories, escalate the issue to a higher group, internally or externally. Your goal is always to resolve the issue.

### *Establish a plan of action to resolve the problem*

Once you have identified the source of the problem, look at the options available to resolve it. In some cases, you will be working on a problem with a small scope, while at other times you will be dealing with a widespread problem.

When the scope is small, your testing may result in having a fix implemented, while in widespread problems, your fix may only correct the problem on one system or a small part of the overall infrastructure. It is also possible that your fix was only implemented in a lab environment when you were testing your theory. When your testing only corrects a test system or a small part of the infrastructure, you will need to create a plan to apply that fix to the rest of the affected devices or components.

When you create your plan to resolve the issue for all systems, it may take the form of a multi-step action plan, with many devices or administrative users being required to implement all the steps. Look at the pros and cons of different approaches and present them to your customer or management. You will usually have several available paths to reach the same end.

## ***Verify full system functionality***

Once you have implemented your fix to the affected systems, you will need to verify that the system is actually back to proper functionality. This may require the affected users, as well other users, to test functionality. The process used to confirm functionality as well as a definition of what is to be considered full functionality can be integrated into your plan of action.

## ***Implement preventive measures***

Once you have found the problem, resolved it, and verified that the system is back in full operation, what else can you do? Well, if that problem was a result of user error or malicious people, then take a minute to think if there is anything that can be done to prevent the problem from re-occurring. You usually cannot remove all chance of it happening again, but you may be able to take some steps that will greatly reduce the chance of it happening again. For example:

- » If the problem was related to malware being installed from a website, then anti-malware software could be installed.
- » If the problem was a dropped laptop, then a proper carrying case can be provided.
- » If the problem was a file that was modified or deleted, then you can adjust the security or permissions on the file to prevent it from happening again.

By helping your clients this way, you may not see them back with the same problem; but this type of action will increase the level of trust between you and the client, which will bring the client back to you in the future.

Going the extra mile also involves contacting the client in the near future to ensure that your work properly resolved the issue and that he or she is happy with the service you provided.

## ***Document findings, actions, and outcomes***

The philosopher George Santayana said, “Those who cannot remember the past are condemned to repeat it.” To remember a solution for the long

term, write it down or otherwise record it. If you do not document your findings, you might find yourself repeating the same troubleshooting steps in the future to solve a similar problem, when the process could have been abbreviated.

I recommend using a personal or a corporate knowledge base to record troubleshooting activities and incident documentation. Some companies have a formal help desk or trouble ticket system, with the main goal of documenting their problems and solutions. Having a technician close his trouble tickets with “Problem resolved” might be fast for the technician, but it is not the purpose of the application. One of the application’s goals is to build a database of problems and resolutions. The more detail that is included in the resolution documentation, the more helpful it will be in the future.

After the trouble ticket database has enough information, it becomes more than a place where the information is stored: It also becomes a place where solutions are found. The larger the database, the more likely it will be able to provide your solution. When a problem is reported, you can search the database to see whether the problem has previously happened for that person (or another person), and you might be provided with a solution. Testing a few known solutions is faster than starting the troubleshooting process at the beginning.

Depending on your job role, you may also need to document the solution for your clients, so that they have a permanent record of the fix or a record of how you spent your time.

## DOCUMENTATION RESOURCES

CompTIA A+ Certified Professionals aren’t expected to know every answer, but they should have a good list of resources at their disposal to find an answer. Here are the most common resources:

- **Network topology diagrams:** When troubleshooting network issues, the best source for information is the networking documentation, which will include network topology diagrams. These diagrams should include

information such as network segments, IP addressing, link speeds, and device locations.

- **Searchable knowledge base:** In the same way your organization can create its own internal knowledge base of problems and solutions, many vendors have compiled their knowledge bases, and they make this data available and searchable on their websites. If the manuals seem to be lacking, see whether the vendor has a searchable online knowledge base. In some cases, vendors ignore the manual when they maintain a good knowledge base. In the case of Microsoft security patches, Microsoft maintains a knowledge base of articles, which have IDs starting with the letters KB.
- **Incident documentation:** Incidents are part of a modern help desk or incident management system. Information Technology Infrastructure Library (ITIL) and IT Service Management (ITSM) both have definitions of incidents and incident management. An incident is an unplanned interruption or reduction in an IT service that may or may not have impacted a user of the service. If a website goes offline unexpectedly for 30 minutes and is restored to service without users knowing, it is still an incident. Documenting the incident, the detection, and the resolution is important in both the management of that incident, as well as future incidents.
- **Regulatory and compliance policy:** If your organization must adhere to government regulations, there should be appropriate internal policies to ensure that all employees follow the appropriate regulations when carrying out their work duties. Most governments have many regulatory bodies representing the different government regulations, and failure to remain compliant with those rules will have penalties that can affect the future of the organization.



- **Acceptable use policy:** Acceptable use policy refers to the use of company equipment you are provided to carry out your job. Is it acceptable to do your personal banking from your work computer? Is it acceptable to use your work cell phone for personal calls? Or book movie tickets on your work cell phone after hours? Those are good questions and they may — and should — be referenced in your organization's acceptable use policy.
- **Password policy:** The organization's password requirements should be available to an employee in the form of a password policy that documents the length, complexity, and age requirements for different systems in the organization. Adherence to the policy may be ensured by IT systems that have the ability to enforce the stated policy. For example, Active Directory has a password policy that ensures users adhere to password complexity guidelines, but your telephone system may not have the same ability to enforce voicemail passwords. Similarly, there may be no way to enforce that users have unique passwords on different systems on your network, but your written policy may indicate the requirement.
- **Inventory management:** Documentation related to inventory management allows you to know which items an organization owns, as well as where they are located or who has them. Each organization will determine what value or type of asset needs to be tracked and to what level it needs to be tracked. Typically, higher-valued assets, such as computers and monitors, are tracked, but smaller items such as mice and keyboards might not be tracked. Tracking involves recording the asset information, such as the make, model, and configuration in a database. To keep these assets organized, typically each asset is assigned a unique number, and in most cases, this number is affixed to the asset with an asset tag. The asset tag may include both the number and a barcode of the number to allow for faster

inventory processing by scanning the assets rather than manually typing in the asset number.

- **Vendor manuals:** Gone are the days of an IT department filled with bookcase upon bookcase of manuals for every application the company owns. In many cases, manuals are now shipped on DVD in PDF format or are available for download from vendors' websites. Many of these manuals have specific sections detailing product installation, options to watch during the installation, and diagnostics or troubleshooting. Looking up a computer's symptoms in this guide can lead to concise, quick solutions.
- **Service documentation:** In addition to general user manuals, some companies offer additional service documentation that can be obtained by owners of the product. In some cases, this will be available to you only if you are certified on the product or you are employed by the manufacturer. Check whether this technical documentation is available to you because it often has detailed configuration and troubleshooting information.
- **Training:** Knowledge is half the battle, and one of the best ways to get quick knowledge is to attend vendor training on the products that you are working on. In many cases, you will find out a product's *gotchas* — those common but hard-to-solve problems that are unique to the product. If you don't walk away with this, you should at least leave the training with a complete picture of how the product is supposed to work, which can reduce your troubleshooting time.
- **Other Internet resources:** In addition to the vendor websites as an official support tool, additional discussion forums and websites might have answers to your specific problems, even though the website or forum is geared toward a general industry area. For instance, you might have issues with a specific sound card; if the vendor's

website does not provide you with the answer, you might find the answer on a site that covers all computer audio cards and issues. Your favorite search engine is a good place to start looking for these sites.

With these documentation resources and the basic troubleshooting guidelines in your arsenal, you should be able to approach problems and troubleshoot them in a methodical, organized way.

Additional troubleshooting processes for specific hardware components are covered in other sections of this book, with much of it in Book 4, [Chapter 2](#).

## *Implementing Change Management*

Some people are intimidated when they hear the term *change management*, but they shouldn't be. Change management simply refers to the process used in an organization to approve and track changes. Change management can apply to many areas of a business, but in most cases when people refer to change management, they are referring to IT change management. It does not have to be a complicated process.

A change may affect hardware, networking and communications equipment, software, or operating systems, and management of those changes require documentation regarding the change and its process, approvals, contingencies in the event of failure, and a post-installation summary.

A change management process benefits an organization in many ways such as:

- » Reducing the time it takes to implement the change
- » Reducing risk during the change
- » Increasing rates of success
- » Enabling the anticipation of challenges and planned responses

The change management process is a documented business process, like many other business processes, such as purchasing equipment or hiring an

employee. There is a standardized and documented process to follow, which may involve forms, approvals, and verifications. In the case of the change management process, the documentation typically starts with a Request for Change (RFC), which is a document that should contain the following pieces of information:

- » Purpose of the change
- » Scope of the change
- » Risk analysis
- » Plan for change
- » Backout plan
- » End-user acceptance
- » Change board results
- » Document changes

The rest of this section will review each of the items of an RFC in detail.

### ***Purpose of the change***

The first and foremost piece of information in the RFC document, which starts the change management process, is the purpose or reason for the change. This reasoning is used by the Change Advisory Board (CAB) to determine if the change should be allowed.

### ***Scope of the change***

The scope of the change represents the items that will be changed and who or what will be affected by it. If it is an Active Directory Group Policy Object (GPO) change, it would affect all desktops and servers on your network, while a change to an SQL server may only affect the applications that use databases on that server. You can read more about Active Directory GPOs in Book 9, [Chapter 2](#).

### ***Risk analysis***

The risk analysis evaluates both the risk of making the change and the risk of not making the change, as both courses of action may have negative

consequences associated with them. One such change that comes to mind is monthly patching of servers, where patching may cause an issue with a specific application, while not patching may leave you in a vulnerable security position. There is risk to either action, which should be spelled out in the risk analysis part of the RFC.

### *Plan for change*

Planning for the change is one of the best options for risk reduction. The more planning you do for a change, the less likely there will be an interruption in service or functionality when the change is implemented. For some changes, this may mean applying the change to group of systems on the network, or a full-scale test of the change in a lab or test environment. The more time spent on the planning section of the RFC typically means the less time you will spend on implementing the actual change.

### *Backout plan*

In most organizations, to go along with the documented and tested plan for implementation, it is important to have a backout plan. The backout plan is also a tested plan that can be used to reverse the changes if there is a problem. This may involve removing a piece of hardware and putting the old unit back in place, restoring a system from a backup, or uninstalling an update. The change follows standard implementation steps, such as backing up a server and verifying the backup before going ahead with the change.

A time factor usually triggers the backout plan, such as the length of the change window divided in half. If the change is not implemented, tested, and validated by halfway through the change window, you will start the process to roll back the change. In some cases, the rollback is as quick and simple as turning off the new server and starting up the old server. In most cases, people will tend to run the clock out on the change before implementing the backout plan, as it means they will need to wait for the next change window to make a second attempt at the change.

### *End-user acceptance*

In many organizations, systems are maintained by IT, but they are used by and sometimes “owned” by end-users or departments. If a change is going to affect an application used by a group, that group should be made aware of the change, the impact of the change, and the potential risks involved with the change. Since it is the end-user who will be affected, some changes require that end-user to accept the change. If you are planning to upgrade the version of SQL Server running all of your corporate databases from accounting to payroll to sales, then all of those departments are the end-users of the database, and all of them will need to accept the change. While you may have established maintenance windows when you are able to apply the change, the actual change needs to be approved, especially if it needs to happen outside the established maintenance window.

## ***Change Board***

With end-user acceptance out of the way, the change can then go to the Change Advisory Board (CAB) or “[Change Board](#).” This represents the main approvals process. The CAB typically includes representation from most major departments in the organization, including management and IT, and representation from the end-users (often done by the Help Desk, as they will be getting the calls from the end-users). The CAB will review the RFC and determine if there a need to proceed, and validate that there is a proper implementation and backout plan in place.

Usually the CAB only meets one or two times a month, so changes are typically planned well in advance. However, there is usually a process in place to deal with emergency changes, such as when you need to reboot the server to resolve a particular issue. The emergency change process would be used as a notification process that an action needs to be taken, may have an abridge approval process, and would typically have a post-mortem during the next CAB meeting.

In some organizations, there are classifications of changes, as well as classifications of resources, such as servers, that will affect the change management process. For example, servers may be classified as Testing, Development, Acceptance, and Production, where Acceptance and

Production may have stringent change management with lesser processes for Testing and Development.

There may also be different processes based on the type of change, such as standard and non-standard changes, where it may be enough to publicly schedule and record that a standard change occurred, and it does not need to go through the change management process. A standard change may include applying security updates to a server, which are scheduled on a change management calendar and applied during a standard maintenance window. This record keeping allows for anyone responsible for that server to be aware of the change, and if that person is troubleshooting a new issue on the server, to be aware that there has been a change to the server. Other changes in the environment may not require change management at all and may follow standard processes, such as the creation of new user accounts, which may involve creating a shared folder on the server to hold their home directory.

What constitutes a change and the processes to follow when a change is made is part of each organization's IT procedures. It is important that there are processes, and that everyone is aware of them.

### *Document changes*

After any changes are made in your organization, it is important to record those changes so that you maintain current documentation related to the configuration of your IT systems. Documentation of the change represents the last step in the process, and your documentation can include a reference to the RFC, which should include the results of the change, stating whether it was successful or unsuccessful.

## *Professionalism and Communication*

Whether you are an internal or external support professional, you have customers. For the external support professional, it is easy to identify your customers. For the internal support professional, the people for whom you provide support are still your customers, and you still need to provide

them with service. To provide this service, you will be required to communicate with them, and this communication should remain professional in its tone and manner. The best way to maintain the right level of professionalism is to respect the customer; whether the customer is right or wrong, you should still give him respect. You can show him respect while you educate him, work with him, or explain to him what he doesn't understand related to the technology that he is using.



FOR THE  
EXAM

The professionalism and communication section of the A+ Exams should be common sense for most readers. The exam questions will present a wide range of responses to given scenarios; the answer will usually be the one that illustrates good communication skills and respect for the client. Verbally abusing the client and hanging up will not be the correct answer!

## ***Good communication skills***

*What we've got here is a failure to communicate.*

— COOL HAND LUKE

A breakdown in communication can be blamed for many of the problems that exist in our world today. Difficult customers or situations are a source of conflict, but that conflict often begins with a misunderstanding. To avoid this conflict with your customers, always make sure you use good communication skills. Here is a list of things to keep in mind when communicating with a customer:

- » **Listen to the customer and don't interrupt.** One of the best abilities of a good communicator is the ability to listen. All too often in today's society, the emphasis is on speed; and for the sake of speed, people tend not to listen. The active part of "active listening" is still listening and may include taking notes. Part of "not listening" is completing other peoples' thoughts or sentences. This is a problem that can be resolved by resisting the urge to just jump in and taking notes to discuss after the customer has finished her statement. Put yourself in



the listener's position while you let the person tell you the problem and how it is affecting her life. "Not listening" can extend to email. I have written emails to vendor support addresses, detailing a problem and the steps already taken to solve that problem, only to receive a stock reply from the vendor support person saying, "Try this," which was already tried, or does not address the problem. At times like that, I usually reply to the email, stating the fact that he failed to read message and rather suggested a solution based on the subject line or the first line of the message.

- » **Clarify statements and repeat what you have heard.** One technique that helps to clarify any misunderstandings is to repeat to the user what he told you. This reinforces for the user that you are listening and are not daydreaming. It also verifies that you understand what the user said. When you restate the issue, you may substitute terms or give additional examples of what the client described to you. Ask questions to gather additional information about what the customer is saying.
- » **Use open verses closed questions to gather information.** Open-ended questions will encourage the customer to provide additional information, rather than closed-ended. A question such as "Describe what you saw," is better than "Did the screen flicker?" You may get information you did not expect when using open-ended questions and this may help in narrowing the scope of the problem.
- » **Use clear, concise, and direct statements.** Translation: Don't be long-winded. Many people like to hear themselves talk; resist any temptations to verbosity you might have. Don't use a \$10 word when a 25¢ word will do. Keep your statements direct with clearly focused points.
- » **Avoid tech talk.** As a CompTIA A+ Certified Professional, you are constantly exposed to technical terms and abbreviations that you slowly incorporate into your vocabulary. However, not everybody in the general public is familiar with *RAID*, *asynchronous*, *MTBF*, *SCSI*, and a whole slew of other terms can confuse clients who refer to the computer as being composed of a monitor and a hard drive. Whenever

possible, try to gauge the user's knowledge level and use an appropriate level of terminology. If you think the user will not understand it, avoid the jargon, acronyms, and slang.

## *Professional behavior*

Always try to conduct yourself with professionalism. Doing so generates respectability in the eyes of your clients and supervisors. The following list contains some aspects of professionalism that should be practiced:

- » **Positive attitude:** It is often said that animals can smell fear on a person. The same is true of users: They can smell a negative attitude right away. You should approach each client and each job with a positive attitude and a feeling of confidence. If you do, you will get more satisfaction from your job. Regardless of your position, there will likely be some aspects of your job that you don't enjoy, but don't let these things bring down your attitude.

In most cases, you deal with clients who have problems that might put the client in a foul mood. If you seem happy to see a client, he will likely lighten his mood, and you will both have a more positive experience. Win/win.



**WARNING** This could go in reverse if you let it: The client's negative attitude could dampen your mood. Don't let this happen. Stay positive.

- » **Project confidence:** As with a positive attitude, it is important to project confidence in your role as a CompTIA A+ Certified Professional. Having confidence in your actions is important to establish trust with your customers and to increase their confidence in you. This does not mean that you always need to know the answer; but it does mean that you need to be confident even when saying you do not know. You are always able to tell the customer you will find the answer for him.
- » **Proper dress:** Professionalism likely includes appropriate attire as well as attitude. When choosing what to wear, plan around the jobs

you are doing. Client meetings might dictate formal business attire; if you are expecting to pull cable through crawlspaces, though, something more casual would fit the task.



**REMEMBER** Regardless of the job, your clothes should be clean and well-kept. To a client, a shoddy appearance indicates shoddy work.

» **Privacy, confidentiality, and discretion:** It's surprising what information clients are willing to let you see on their computers. In many cases, you have access to their most private documents. In corporate environments, this can include confidential employee information found on the computer you are servicing, documents left in a printer, or documents and material left on the desk at which you are working. When doing retail bench work, this can include private financial information that is in their computer. A client's computer often holds information that you should not be seeing — and, in normal circumstances, you would not be allowed to see. In most cases, you will know what you should and should not be looking at. If there is a reason to open a file to verify accessibility, then sure — you will need to do that. However, you should ignore the information you find when you're done. Here are few additional key items to remember when dealing with this topic when working as outside IT professional:

- Some companies have high standards when sharing information with you, and may have issues with you accessing any data on the computer — especially if you will be unsupervised. Be cognizant of this, and ask permission before continuing if you think there may be a concern.
- If customers express concern in respect to your access to data, take steps to put them at ease.
- Be familiar with government regulations that may affect your data access requirements related to their customers' personal

data. Some industries, such as healthcare, have very stringent guidelines.

- Check your own company guidelines on data access and retention, which may be more strict than the customer's own guidelines.
- Do not confuse the line between customer confidentiality and the law. There are no client-IT professional privileges, so if you stumble over something that is illegal, you are obligated to report it to the appropriate authorities.



**WARNING** As an outside consultant, I am amazed by the number of clients who freely offer up administrative credentials for their network, granting access to all areas of the network and to all kinds of information. Take care to ensure that these credentials are not misused by you or put in a place where they could be used by another person without your knowledge.

- » **Social media:** If you are going to respect your customer's privacy as you just read, that means you should never post information about your customer or your experiences with your customer on any social media sites. That should go without saying, but with many people I know, it does need to be said, and then said again. Many companies have people who are given the job of monitoring the company's references in social media, so what you are saying may get back to the company, even if you think you are using a private or semi-private medium. In the worst cases, dismissal or a lawsuit may be the result. The best words of advice I have for you, were given to me early in my online life: "Never put anything into an email (or social media post, tweet, blog, vlog, or whatever) that you would not want to appear on the front page of a newspaper."
- » **Expectations and timelines:** Many issues may arise from a different level of expectation between you and the client. Make sure that you set or agree upon expectations, and work to meet or exceed them:

- If a variety of service, repair, or replacement options are available, discuss them with the client and ensure that the client knows which one you will be working on.
- If you need time to perform the work, set the expectation as how long it will take and, if something happens to change the time, make sure to follow up with the client and communicate the status, reason for the delay, and new expected completion time.
- Always ensure the client receives proper documentation related to the work that was performed or the services that were provided.
- You should follow up with the client after the service to ensure that the repair work was satisfactory and that the problem did not return.

» **Respect:** People with different cultural backgrounds will have different means of showing respect, and you should use techniques appropriate to your local region or culture. In general, the techniques listed here are fairly universal. Respect should be thought of as a two-way street. In most cases, if you show appropriate respect to your clients, they will return that level of respect.

If the client doesn't show you any respect, stay calm and continue to be respectful. Ask the client to calm down and tell him that you will not be able to help if he does not give you the information you need. This is a tough situation to call because when people are told that they are not acting appropriately, they either calm down or become defensive and more disrespectful. While you tell them that they should calm down, make sure to reinforce that you want to help them. The logic of the situation might finally sink in.

Some steps or actions you can take to show respect are

- *Don't argue or be defensive.* The client might be in a foul mood. You would likely be as well if technology got in the way of your job or you thought that you had just lost several years of

personal data or photos. A client might have many reasons to be upset when you start dealing with him.

To some clients, you represent the technology they're having issues with. Their frustration often gets vented all over you. Don't take this personally or get upset by users' actions. Do what you can to relieve some of their stress and remind them that you're not part of the problem. Rather, you're part of the solution.



**REMEMBER** If you argue with the client, the entire issue will most likely become ugly. Avoid arguing at all costs.

- *Don't belittle, dismiss, or minimize problems.* In most cases, the problems that users face are serious to them. Even though you might not share their view of the importance of the problem, do not dismiss the issue. By claiming that the problems are trivial, you suggest that the clients' feelings are trivial. If the clients were not upset before this point, they will be if they think you are trivializing them.
- *Don't be judgmental.* Any biases you have should be checked at the door when you come to work. That way, you will likely reserve your judgments on issues until you have seen all the facts. This point goes very nicely with the previous one: namely, that if you pass early judgment on a user, you might be more inclined to trivialize her issues.
- *Avoid distractions and interruptions.* When dealing with a client, try to reduce distractions for yourself. If you are working a help desk, you should not be carrying on conversations with coworkers around you when you are on a support call. If you are working a retail repair bench, you should deal with one client at a time and not try to multitask among them or take phone calls. If you are visiting a client, you should silence your cell phone and not take calls, text

messages, tweets, or use other social media tools. Eliminate all personal interruptions.

In all cases in which you are physically with a client, maintain eye contact. This will be taken as a sign that you're paying attention. If you don't maintain eye contact, the client will think that you are not paying attention. There is also a chance that you might become distracted by something you see. If you maintain eye contact, you will not get distracted by other events, and you will tend to have a better understanding of what is being said to you.

- *Be on time.* It is a good practice to plan your trips to a client site to arrive early. I once had a boss who told me, "If you are not 10 minutes early for your appointment, then you are late." By planning to arrive 10 minutes early, even if something happens on your trip, you may still be able to be on time for that actual appointment. If something happens and you will be late, then contact the client with as much notice as possible. When I started in this industry, you did not have an option to easily contact the client while in transit, but in the current well-connected world, the client can be contacted via multiple methods (email, text, or phone call) while en route. When you know you are going to be late, let the client know.
- *Property is as important as people.* Respecting the person extends to respecting his or her property and privacy. For many clients, you will be working in their office, very possibly at their desk. When you're waiting for a reboot or for software installation, you will be tempted to look around. Don't do it! You should always respect your client's privacy and possessions, from the computer to the Marvin the Martian action figure.
- *Don't bad-mouth other clients.* Respect for a customer extends beyond the time you spend fixing his computer. Don't be disrespectful of any client in front of current ones. If the client sees you lack respect for others or hears you say negative

things about other clients, she will think that you are going to say similar things about her to your other clients.

- *Be culturally sensitive.* With the globalization of IT services, as well as the multicultural makeup of so many countries, you will invariably be working with people from different backgrounds and ethnicities. Some care should be taken to avoid offending the people you will be dealing with, either as customers or fellow employees.

With the wide range of customs that you may encounter, this may not be possible all of the time; many of the colorful expressions that we have grown up with may be taboo.

Whereas some of these remarks that we make can sometimes be thought to be colorful, it is easy to cross the line, in some cases without ever planning to. I once began describing a problem where only one control process should talk to the system, and used the expression “Too many chiefs ...,” and stopped there, realizing that I was working with a group of Native Americans; I have not used that expression since, opting instead for “Too many cooks ...,” and fewer hurt feelings.

Another way to display cultural sensitivity is to use proper titles when addressing customers. Many cultures have rules around the use of given and/or surnames. For example, in Chinese culture it is customary to always use the surname, but never alone.

## *Getting an A+*

In this chapter, I discuss general skills that will make you an effective troubleshooter, as well as how you present yourself to and treat the clients that you deal with. The following points are covered:

- » Create a list of possible problems based on the information that is provided to you, and then follow that up with testing to locate the true cause.



- » When troubleshooting problems, work through systems sequentially from general to specific or from beginning of a system to its end. That way, you won't miss items that may be involved in the solution.
- » Back up user or system files and any configuration files or settings that may be lost or changed during troubleshooting.
- » Document issues, solutions, and any other items that are important.
- » Follow basic principles of inter-personal respect, which will answer most exam questions related to professionalism and communications.
- » Implement change management, including creating an RFC document, which should include the purpose of the change, the scope of the change, a risk analysis, the plan for the change, a backout plan, and end-user acceptance.

## *Prep Test*

- 1. Which of the following is *not* a step in the basic troubleshooting process?**
  - (A) Document findings
  - (B) Respect client property
  - (C) Evaluate results
  - (D) Identify the problem
  
- 2. Where should you go to get a complete list of problem symptoms?**
  - (A) Product documentation
  - (B) Internet search engines
  - (C) Question the user
  - (D) Analyze the problem
  
- 3. Which of the following should you find out when questioning the user about his or her computer issue? Choose the best answer.**
  - (A) Recent changes to the computer

- (B) The last time the computer was shut down
  - (C) How the computer is connected to the building's electrical system
  - (D) The location of resources to document your outcomes
- 4. When making configuration changes during the troubleshooting process, what practices should be followed? Choose all that apply.**
- (A) Apply one configuration change at a time
  - (B) Discount the obvious
  - (C) Back up any settings or files that you need to change
  - (D) Test related components
- 5. Which of the following are key items belonging to the Request for Change (RFC) document? Choose all that apply.**
- (A) Purpose of change
  - (B) Potential fixes
  - (C) Change administrator
  - (D) Backout plan
- 6. What is the purpose of the Change Board?**
- (A) Store a list of approved changes
  - (B) Implement the change in the organization
  - (C) Approve changes within the organization
  - (D) Create the RFC document

## ***Answers***

1. **B.** Respecting client property is part of good communication skills, not the troubleshooting process. *See "Using Troubleshooting Procedures and Good Practices."*
2. **C.** The best source for finding out what the symptoms are, and a description of what appears to be wrong with the computer, is directly

from the user. *Review “Identify the problem.”*

3. **A.** The user should be questioned about changes that have been recently made to the computer. In some cases, a user may not know or may not want to tell you. *Check out “Identify the problem.”*
4. **A, C.** Before applying any changes to the system, relevant files and settings should be backed up so that the changes can be reversed or critical files can be restored if anything goes wrong. You should apply only one change at a time so that you will know what change actually resolved the problem. Although testing related components is part of the overall troubleshooting process, it does not necessarily apply to making configuration changes. You should not discount the obvious. *Peruse “Using Troubleshooting Procedures and Good Practices.”*
5. **A, D.** The purpose of the change and backout plan are both part of the RFC document. Potential fixes are part of the troubleshooting process. Change administrator is made up, but each RFC document usually identifies the owner of the change, who is typically the person who has initiated the change and files the RFC. *Peruse [“Implementing Change Management.”](#)*
6. **C.** The Change Board is responsible for reviewing and approving proposed changes. These changes will be initiated and carried out by other people in the organization. *Review [“Implementing Change Management.”](#)*

## Chapter 3

# Protecting Yourself and Your PC

---

### IN THIS CHAPTER

- » Gathering the tools of the trade
  - » Understanding ESD and EMI
  - » Personal safety and high-voltage equipment
  - » Disposing of components
  - » Understanding ergonomics
- 

Before addressing how to install computer components such as memory, processors, or a hard drive, you want to make sure that you understand the risks that are involved every time you take the cover off the computer. On the A+ exams, CompTIA will be sure to test your knowledge on how to safely handle a computer's electronic innards and how to safely and legally dispose of broken or obsolete parts.

In this chapter, I discuss ESD (electrostatic discharge) and EMI (electromagnetic interference), as well as what high-voltage equipment is and why you should stay away from these components. I also show you how to dispose of computer components, and then introduce you to ergonomics.

## *Gathering Tools of the Trade*

When plumbers or electricians come to your house to do some work, they bring a toolbox containing what they need to fix most problems that might arise while on the job. As an A+ Certified Professional, you need to do the same thing: Keep a PC repair toolkit of all the tools — software and hardware — that you need to do your job.

The following sections discuss the hardware and software tools that you need to perform your job well.

## *Hardware tools*

Of the myriad pieces of hardware you need to repair computers, the most popular is the humble screwdriver. You can purchase a PC repair toolkit (shown in [Figure 3-1](#)) at your local computer store, but you should be able to get away with a multihead screwdriver for most jobs.



**FIGURE 3-1:** A typical PC repair toolkit.

The following is a list of tools that you might need from time to time to fix most of your computer repair problems:

- » **Screwdrivers:** Most toolkits come with a variety of screwdrivers that have a variety of tip shapes and sizes — flat-head screwdrivers with a flat tip, Phillips screwdrivers with a +-shaped tip, and TORX screwdrivers with a star-shaped tip. I usually use a multihead screwdriver instead of choosing from a mass of different screwdrivers.



**WARNING** Be sure that you don't use a magnetic screwdriver on the computer because you could erase your data!

- » **Tweezers:** PC repair toolkits typically come with a set of tweezers, which are a lot more useful than they might seem. You use tweezers to work with smaller items in the computer, such as jumpers. (For more information on jumpers, check out Book 2, [Chapter 1](#).)
- » **Chip extractor:** A lot of PC repair toolkits come with a *chip extractor*, which you use to remove a chip from a board. For the most part, you won't need this tool because most of the chips today are on a card or module instead of being attached directly to the board: You can remove the entire module by hand.
- » **Chip inserter:** PC repair toolkits also come with a *chip inserter*, which you use to push a chip into a socket. This tool is just as useful (or useless) as a chip extractor.
- » **Canister:** A number of premade PC repair toolkits include an empty canister, which seems really silly at first but becomes very useful. You can use this canister to store additional screws or jumpers. Before throwing away any old computer parts, I usually take the screws and jumpers off and put them in my canister. You never know when you might need them!
- » **Multimeter:** You can use a multimeter (shown in [Figure 3-2](#)) to verify that the wall outlet is supplying the correct voltage and that your power connectors to the hard drive and CD-ROM drives are supplying the correct voltage as well. This is a useful tool to have around if you suspect the power supply isn't doing its job.



**FIGURE 3-2:** A digital multimeter can be a valuable tool when troubleshooting power problems.

## *Software tools*



Most technicians think of hardware tools when they think of tools of the trade, but software tools are important, too. I give you in-depth information about the software tools you need in your PC repair toolkit in Book 6, [Chapter 4](#), but I want to introduce them here so you get a more complete listing of the tools you will use in the field:

- » **Windows DVD:** The Windows DVD can help you fix boot problems with Windows when a file goes missing. You can also use it to recover from some basic disk problems by using the Recovery Console.
- » **Live DVD/flash drive:** *Live DVD* is the general term used for booting and running the operating system from DVD. There are Live DVD versions of Windows and Linux, and you can use them to help retrieve your data when the operating system will not boot. You can also run these live operating systems from a thumb drive as well.



**REMEMBER** These are just a few of the software tools that you can use. You find out more about troubleshooting utilities found in Windows by checking out Book 6, [Chapter 4](#).

## *Avoiding the Dreaded ESD*

In this section, I discuss the dangers of servicing a system without taking precautions as to not damage the computer or hurt yourself. Be sure to take this section very seriously!

### *ESD means electrostatic discharge (not extrasensory deprivation)*

When you walk around on carpet, scuffing your feet, you build up a static charge. You walk over to your best friend, touch his or her hand, and zap! — an explosive shock! You feel that static shock because you have a higher static charge than your friend. When two objects with dissimilar



charges touch, the excess electrons are transferred to the object with the lesser charge. This is when you feel the shock.



**TIP** Here comes the important part: *That little shock is more than enough to kill a computer chip.* So, had you touched a computer component instead of your friend, you would most likely kill the poor little computer chip.

The scary part about all of this is that in order for you to feel the shock, you must have a charge of approximately 3,000 volts (V), but only about 200V are needed to kill a computer chip — and just 30V can do long-term damage to a chip.

Transference of static charge to another object — *electrostatic discharge (ESD)* — is responsible for damaging or killing computer components, such as computer chips. It is your job as an A+ Certified Professional to make sure that you eliminate ESD by following ESD best practices.

## ***Component handling and preventing ESD***

When handling computer equipment, it is critical that you know how to handle computer components to prevent the destruction of the equipment with ESD by implementing proper equipment grounding techniques. You can reduce ESD, but because ESD occurs naturally, you can never completely get rid of the static buildup you carry with you. To reduce your chances of damaging a system when servicing a computer, follow these best practices:

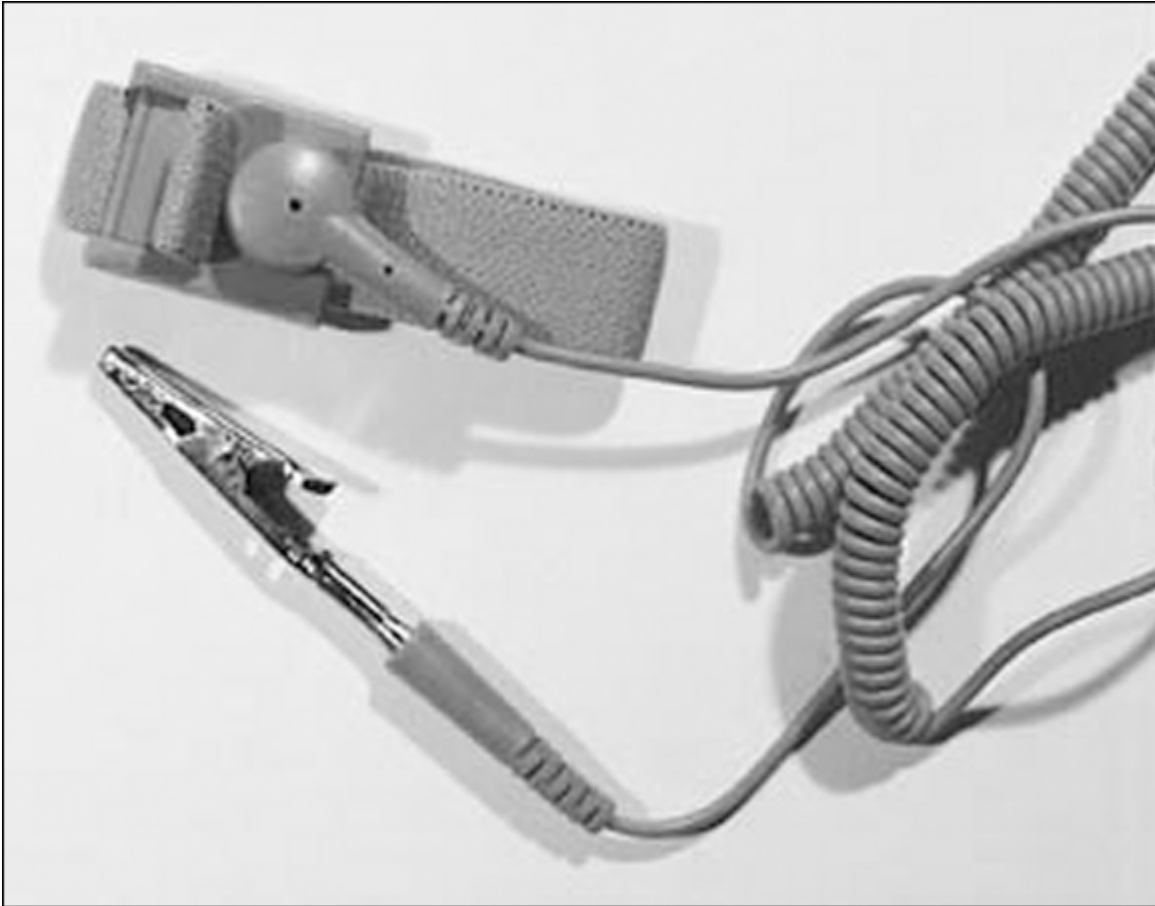
- » **ESD straps:** One of the most popular solutions for preventing damage to computer components is to wear a grounding strap (shown in [Figure 3-3](#)), which is also known as an *ESD wrist strap*. The grounding strap goes around your wrist and contains a *resistor* that absorbs any static electricity. The wrist strap then clamps to the metal *chassis* — the casing — of the computer. This gives you constant grounding while servicing the computer, eliminating any static buildup.



TIP

If you don't have a grounding strap to connect to the chassis of the computer, be sure to constantly eliminate any static electricity that has built up on yourself by touching the chassis before touching any computer part. Keep in mind that you should always disconnect the power from the computer before working on it.

- » **ESD mats:** You can also prepare an ESD workstation using an ESD mat. The ESD mat connects to the grounding plug in the power outlet of the wall and then has a place to connect the workstation to the mat to get the ground.
- » **Carpet spray:** You can use a specialized carpet spray on the carpet around your work area to help reduce the static electricity, but it won't eliminate the static entirely. Don't rely on antistatic carpet spray as your *only* source to eliminate static electricity.
- » **Self grounding and equipment grounding:** You can ground yourself by connecting a grounding strap to the grounding plug of a power outlet, or purchase specially designed grounding equipment.
- » **Antistatic bags:** When carrying computer components from one place to another, it's a good idea to carry the components in an antistatic bag to protect the components from static electricity. For example, if you are going to carry some memory to a user's workstation, carry the memory in the antistatic bag.
- » **Humidifiers:** You can use humidifiers to place moisture in the air. Your goal is to get the humidity level to about 50 percent. Overly dry environments help create static electricity while overly humid environments could create unwanted moisture.



**FIGURE 3-3:** An antistatic wrist strap, also known as a grounding strap.

## *Watching Out for EMI*

A number of people confuse ESD with *electromagnetic interference (EMI)*, which involves computer equipment receiving electrical interference from an outside source, such as another electrical device or a piece of machinery.



**FOR THE  
EXAM**

Be sure to know the difference between ESD and EMI.

Although ESD often causes permanent damage (if you fry a computer chip, it is damaged permanently), EMI is, for the most part, temporary. For example, if you notice that your monitor display is distorted because you

are getting interference from an outside source, moving the monitor away from the external source should get the monitor back to normal.

That being said, EMI exposure for a long period of time *can* cause permanent damage to computer components.

## *Safety First!*

Before continuing into the world of computer repair, it is important for you to follow some basic safety rules. In the following sections, you find out about some basic rules to follow when servicing computers, but you also discover high-voltage equipment you should stay away from unless you are properly trained to service those components.

### *Personal safety*

You should always follow a number of guidelines when servicing the computer. These guidelines ensure your safety by preventing the chances of you getting electrocuted. Keep the following in mind when you crack the cover of a computer open:

- » **Disconnect power before repairing the PC:** Before servicing the system, be sure to unplug the system from the wall to disconnect the power to ensure you cut electricity flow to the device.
- » **Remove jewelry:** Remove any jewelry because a lot of jewelry is made of metals that act as conductors of electricity.
- » **Lifting techniques:** When lifting computer equipment, be sure to lift with your legs so that you do not hurt your back.
- » **Weight limitations:** Ensure that you are not lifting equipment that is too heavy. Use proper moving equipment for heavy equipment.
- » **Electrical fire safety:** Be sure to have approved fire extinguishers for electronic equipment in areas where you are performing your work. Also test the fire extinguishers on a regular basis to ensure that they work.
- » **CRT safety, proper disposal:** Most computer equipment, including CRTs, can be dropped off at a recycling facility to be properly

disposed of.

- » **Safety goggles and air filter mask:** When working with computer systems that contain a lot of dust, or working in areas that contain a lot of dust, be sure to wear safety goggles and an air filter mask so that you do not breathe in the dust particles.
- » **Cable management:** When working in a networked environment, be sure that all cables are bundled together and not left out in the open where someone can trip over them. You can purchase cable mats that are rubber mats that can hide the cable if you need to have cables running over the floor.

## *Recognizing high-voltage equipment*

*High-voltage equipment* can cause serious injury if you touch it — it might even kill you. You will not typically service these two major computer components unless you have special training or certification beyond the A+ certification exams:

- » The power supply unit
- » The monitor



**WARNING** The danger in servicing the power supply and a cathode ray tube (CRT) monitor is that both devices use capacitors that hold an electrical charge even after the component is unplugged. The electrical charge is enough to cause severe shock or electrocution. Beware!

High-voltage equipment usually bears a warning label that indicates that you shouldn't open the component — and, that if you do, you could be severely hurt. Bottom line: You're playing with fire (all right, electricity) if you open these components. Have them serviced by a certified electrician or someone with special training.

## *Power supply unit*

The *power supply unit (PSU)* is responsible for taking alternating current (AC) from the wall outlet and converting it to a direct current (DC) that is usable by computer components.

The power supply usually takes 120V of alternating current from the wall outlet and supplies the power to computer components by converting the 120 volts AC into 3.3V, 5V, or 12V of DC.

The power supply contains a charge even after it is unplugged, so servicing a broken power supply is not recommended. If your power supply is broken, just replace it.



**FOR THE  
EXAM**

For the A+ exams, remember that a power supply is high-voltage equipment that you should keep your hands — and tools — away from.

### ***CRT monitor***

If you end up in a situation where you are asked to service an old CRT monitor, please beware! The part of the monitor that you need to be aware of is the cathode ray tube itself. Creating the images on a CRT monitor takes a lot of power — typically 50,000V, which is enough to cause you serious harm, if not kill you. Remember that this charge is held even when the monitor is unplugged from the wall: As a general rule, do not open the monitor unless you are a qualified professional (and remember that passing the A+ exams doesn't qualify you to work with CRTs).



**WARNING**

As a general rule, you should never open the monitor! Send it to a qualified professional. Because of the risk of the potential seriousness of injury, opening a monitor is not recommended unless you know what you are doing.



**FOR THE  
EXAM**

For the A+ exams, you need to be familiar with the general steps to discharge a CRT. You would discharge the CRT if you were going to perform some work on the monitor (which I do not recommend unless you are qualified). If you decide to open a monitor, you will notice a heavy wire running along the side of the CRT — this wire supplies the 50,000V. Be sure *not* to touch this wire! If you are going to work on a monitor, first discharge the high voltage. To discharge the CRT of a monitor, you need a *shorting probe*. Follow these steps to discharge a monitor's CRT:

1. **Unplug the monitor and open it.**
2. **Clip the wire on the shorting probe to the metal chassis of the computer.**
3. **Slip the end of the shorting probe under the rubber grommet (looks like a little rubber flap).**

Make sure that you don't touch any other metal parts. You should hear loud popping noises as the high-voltage equipment is discharged.

4. **When the popping noise has stopped, you may remove the probe.**



**WARNING** Note that the general steps to discharge a CRT are here for A+ exam preparation purposes only. It is not recommended to open a monitor for any reason unless you are qualified.

## ***Protecting computer components***

After you have dealt with the safety concerns dealing with yourself, you can then turn your focus to protecting the computer components! The following are some guidelines to know for the A+ certification exams regarding protecting computer components:

- » **Reduce ESD:** To help protect your computer components, be sure to use proper techniques to reduce ESD (discussed earlier in this chapter).
- » **Temperature and humidity-level awareness (environment control):** Ensure that you monitor the temperature and humidity levels in areas that have computer equipment. This includes server rooms that have a number of servers, routers, and switches, which cause the room to heat up. In such rooms, be sure to have proper cooling and ventilation systems installed to prevent the equipment from overheating. You want to have relative humidity levels around 50 percent and a temperature around 70 degrees Fahrenheit.
- » **Protection from airborne particles:** You can help protect the system from airborne particles by ensuring that you have all enclosures properly sealed and are using air filters.
- » **Dust and debris:** You can remove dust and debris from the system by using compressed air to blow the dust off the equipment and a small vacuum to collect the dust.
- » **Component handling and protection:** Be sure to ground yourself at all times to protect the equipment from ESD. Place components in antistatic bags if you are removing a part from the computer.
- » **Electrical fire safety:** As mentioned earlier, be prepared for electrical fires and have an approved fire extinguisher close by.
- » **CRT safety, proper disposal:** In the next section, you find out about disposal of equipment. These days, you can drop off old equipment at recycling facilities.
- » **Compliance with government regulations:** Ensure that you are following all safety procedures to ensure that you are compliant with any government regulations and industry regulations.

## *Handling Toxic Waste*

When you replace an old part from a computer, you have a responsibility to dispose of the old part properly. You are not permitted to dump certain



computer components in a landfill because they are hazardous to the environment. For example, the chemicals in a battery could leak into the water supply and contaminate the drinking water. In this section, you find out how to dispose of certain computer components that can be dangerous to the environment.

Federal and local laws regulate the disposal of hazardous materials; if you break these laws, you could be fined. If you're unsure how to dispose of a certain component, contact your state or province environment regulator office to find out how to appropriately dispose of it. You should also watch for organizations such as schools, universities, and sometimes businesses hosting a recycling drive that allows you the opportunity to get rid of old computer equipment.

You can also contact the U.S. Environmental Protection Agency (EPA) for proper procedures and guidelines on how to safely dispose of computer components. These guidelines are also published on the EPA web page at [www.epa.gov/epawaste/conserva/materials/ecycling/index.htm](http://www.epa.gov/epawaste/conserva/materials/ecycling/index.htm).

## ***Batteries***

Because batteries contain metals that are environmentally harmful (such as nickel and cadmium), federal, state, and local laws prevent people from dumping their batteries in trash cans and throwing them to the curb destined for a landfill. The federal government passed the Battery Act in 1996 to ensure that the public properly disposes of rechargeable batteries and batteries that contain mercury. You can find information about the Battery Act by checking out

[www.epa.gov/wastes/conserva/materials/ecycling](http://www.epa.gov/wastes/conserva/materials/ecycling).

Each state has different regulations and rules that deal with the disposal of batteries, and you should be sure that you follow these rules when disposing of old batteries. Contact your state's environmental regulatory office for more information on disposal of batteries and other computer components.

## ***CRTs***

Because CRTs contain harmful components, they cannot be dumped in landfills. You can donate old monitors that are still in working condition

to public schools, churches, and charities. With any donation, you may get a tax benefit! If the monitor doesn't work or is so badly damaged that it can't be given away, you can contact recycling companies that will take it off your hands and use it for spare parts.

### *Toner kits and cartridges*

A number of vendors offer a small discount if you turn in old toner kits or cartridges when you buy new ones. Even if they don't give a small discount, at least they'll take the old toner off your hands. These vendors typically send the old toner kit or cartridge back to the manufacturer to be recycled.

If the vendor you purchase from doesn't take the used toner kits and cartridges, you should contact the manufacturer and find out how you can dispose of them. If you don't want to contact the manufacturer, you can always check with your state's environmental regulatory office.

### *Cell phones and tablets*

The best way to get rid of your old cell phones and tablets is to look for a recycling program in your area. You can find a recycling exchange that takes electronics or you could check with your cellular carrier, as some of them have programs in place that will take your old cell phone and dispose of it for you. Sometime the cellular carrier will give store credit for a new phone if the phone you are bringing in has value.

## *Environmental Impacts and Appropriate Controls*

IT professionals today must be responsible and aware of any dangerous materials that they interact with on a daily basis and how to handle those dangerous materials. In this section you learn about the Material Safety Data Sheet (MSDS), temperature and humidity controls to protect components, power-related issues, and how to keep components clean from dust and debris.

## *Material Safety Data Sheet*

A *Material Safety Data Sheet (MSDS)* contains information about hazardous chemicals present in different materials. The MSDS contains the composition of these materials and includes their ingredients so that you will know what makes up a particular material.

The MSDS also contains information on the proper handling of materials and the lethal doses for each material. You can obtain information on MSDS by visiting [www.osha.gov](http://www.osha.gov) and running a search for “MSDS” and your material.



**TIP**

A great website to find out more on how to donate or recycle computer parts is [www.computerhope.com/disposal.htm](http://www.computerhope.com/disposal.htm).

## *Temperature and humidity controls*

There are a number of issues related to temperature and humidity that can affect the operation of computer systems. Be aware of the following issues:

- » **Temperature:** Having your environment too hot could cause the computers to overheat, which results in the systems crashing or not starting up. Be sure to control the temperature of the environment in which you house the computers — keep the temperature around 70 degrees Fahrenheit.
- » **Humidity levels:** You learn earlier in the chapter that overly dry environments help create static electricity (which can damage computer equipment), while overly humid environments could create unwanted moisture. Be sure to control the humidity levels in your environment and try to keep humidity levels around 45 to 50 percent. You can control the humidity of your environment with a humidifier.
- » **Proper ventilation:** As part of a technique to keep equipment from overheating, you want to ensure proper ventilation of the system by

keeping the fans clean of dust and ensuring that blanking plates are placed over any openings on the back of the system.

## *Power-related issues*

A number of power-related problems can occur that can potentially cause damage to electronic devices such as computers or laptops. You learn more about power in Book 2, [Chapter 6](#), but following is a quick overview of the power-related issues you should be familiar with for the A+ certification exams:

- » **Power surges:** A power surge is a boost in electrical current for a very short period of time, typically less than a thousandth of a second. This additional boost, known as a spike, in power could cause damage to your electrical equipment.
- » **Brownouts:** A brownout is the opposite of a power surge in the sense that it is a shortage of electrical power for a very short period of time. The brownout may occur because the power grid is overloaded. This inconsistency in power can cause damage to your electrical equipment.
- » **Blackouts:** A blackout is a loss of power for longer periods of time. When power is lost, it could cause damage to components or corrupt files that are open. The goal is to protect the system from a power outage with corrective controls, such as battery backups and surge suppressors (which I describe next).

To help protect system components from power surges, brownouts, and blackouts, you can use one of the following two corrective controls:

- » **Battery backup:** A battery backup connected to your computer systems would provide a backup power source for a short period of time, thus allowing you to gracefully shut down the system after a power loss to prevent damage to components or corruption of data.
- » **Surge suppressor:** You can connect your computer systems to a surge protector to help prevent damage from spikes in power, or power surges.

## *Protection from airborne particles*

As I mention earlier, you want to ensure that you are protecting computer components from airborne particles that can get into the system and cause problems, such as clogging up fans, or getting dust in motherboard slots (such as card slots or memory slots) that could cause problems with the cards making clean contact when inserted into the slot. To help prevent issues with airborne particles, use the following:

- » **Enclosures:** Ensure that the computer enclosure is closed and sealed properly. Also ensure that any slots on the back of the computer that are open have dust covers (also known as blanking plates) to prevent dust from getting into the computer.
- » **Air filters/mask:** You can purchase a computer air filter/mask that is placed on the fan to help prevent dust from getting into the fan. This will help extend the lifetime of the fan on the PC.

## *Dust and debris*

If you find you have dust and debris that has built up on the fans or on other components of the computer, you should clean it out. The build-up of dust in the components can restrict airflow, or even cause the fan not to work, which then may cause the system to overheat and become unstable. Use the following to clean the system out:

- » **Compressed air:** You can purchase compressed air from your local computer store to blow out dust from fans and computer components.
- » **Vacuums:** You want to have a small vacuum to collect the dust that you are blowing out of the fan and computer components to prevent the dust from settling on other components in the system!

## *Exploring Ergonomics*

Computers do a lot of great things. They crunch thousands of numbers and process data at phenomenal rates; they perform tedious, repetitive actions without complaining; and they allow a thousand-page book like this one to

be written, edited, and proofread without using a single sheet of paper. Unfortunately, working on a computer can cause health problems.

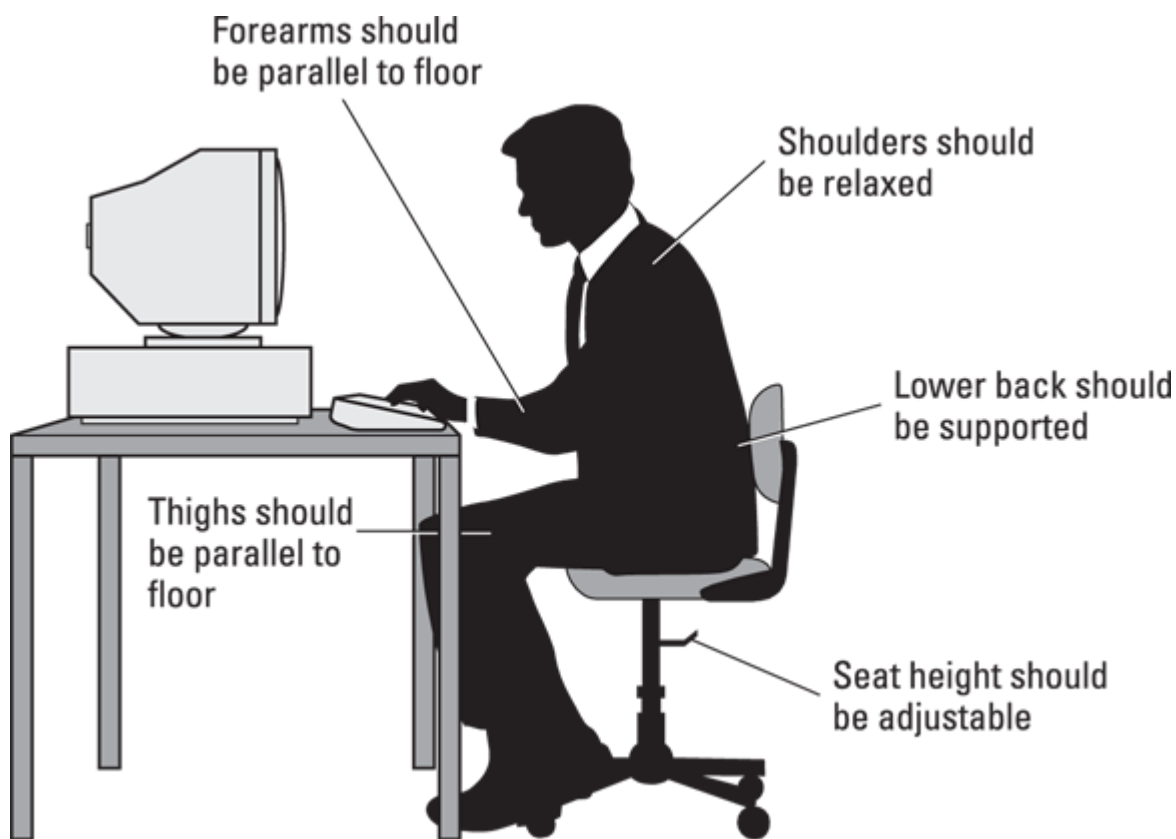
*Ergonomics* is the study, or science, of designing equipment that reduces discomfort for the user and reduces or prevents repetitive strain injury (RSI).

RSI is an injury to the muscles and tendons in the neck, shoulders, arms, wrists, and/or fingers caused by the poor posture and frequent repetitive movements that accompany long hours in front of a computer. Some common examples of RSI are carpal tunnel syndrome, tenosynovitis, and tendonitis. Here are some recommendations you can follow to help reduce discomfort and RSI:

- » **Maintain good posture.** Be sure to keep good posture when working on the computer (see [Figure 3-4](#)). Put your feet flat on the floor; your thighs and back should be at a 90-degree angle from each other; your forearms should be on the table, parallel to the floor.
- » **Use a comfortable keyboard and mouse.** Try to keep the keyboard and mouse at a comfortable position so that you can keep a relaxed posture and not have to stretch too far to do your work. If at all possible, use an *ergonomic keyboard*, which has a left and a right half set at comfortable angles to help reduce the strain put on your wrists, arms, and fingers.
- » **Keep the monitor at eye level.** Keep the monitor at eye level so that you don't have to bend or stretch your neck to look at it. Keep your monitor two feet away from you because of the rays older monitors emit.
- » **Take frequent breaks.** It is so important to take time out in the day to get up and stretch your legs and arms. Staring at the computer screen too long can also hurt your eyes, so give them frequent breaks as well. It's great for the mind, too!
- » **Care for your eyes.** If you are working at the computer for long periods of time, be sure to blink your eyes frequently and try to give them a break by focusing on a distant object for a few seconds every 15 to 20 minutes. Computer users have dry eyes because they don't

blink as often as someone not using the computer all day. Have some eye drops handy when working on the computer for long periods of time.

- » **Use a wrist rest.** If you do a lot of typing and mousing on the computer, use a wrist rest for the keyboard and mouse so that you don't put unnecessary strain on your wrist because of bad positioning.
- » **Invest in a good chair.** If you're going to be sitting for a while, you might as well invest in a good chair. Buy a chair that has an adjustable back and adjustable height and that provides lower-back support.



**FIGURE 3-4:** Having good posture when working on a computer helps prevent injuries to your neck and back.

## *Getting an A+*

This chapter highlights a number of safety issues surrounding the servicing and using of computer systems. The following is a quick review of some of the key points to remember from this chapter:

- » ESD can damage computer chips, so make sure that you do your best to protect computer components.
- » Always use a grounding strap when servicing a computer to prevent damage to computer components from static electricity.
- » EMI is electrical interference from an external source.
- » Recycle computer parts or donate them to charity whenever possible.
- » Power supplies and monitors are high-voltage equipment that holds a strong electrical charge even after unplugged, so send them to a qualified technician to be serviced.
- » Be sure to maintain good posture and use a supporting pad for your wrist if you're doing a lot of typing.

## *Prep Test*

- 1. Which of the following is considered high-voltage equipment?  
(Select all that apply.)**
  - (A) Printers
  - (B) CRTs
  - (C) Power supply units
  - (D) Hard drives
  
- 2. Computer components can be destroyed with as little as**
  - (A) 3,000 volts
  - (B) 200 volts
  - (C) 500 volts
  - (D) 900 volts
  
- 3. Your manager has asked you to take some of the memory out of a system located on the fourth floor and to put it in Jill's computer, which is located on the tenth floor. Which of the following should**



**you use to store the memory module while transporting it to Jill's workstation?**

- (A) ESD strap
- (B) ESD mat
- (C) Safety goggles
- (D) Antistatic bag

**4. Your organization has a number of hazardous materials on site. Your safety manager wants to ensure that the company knows how to handle and dispose of these materials. What should you use?**

- (A) ESD strap
- (B) MSDS
- (C) ESD mat
- (D) Safety goggles

**5. EPA stands for**

- (A) Environmental Protection Association
- (B) Environmental Protection Agency
- (C) Environmental Preservation Agency
- (D) Environmental Preservation Association

**6. RSI stands for**

- (A) Restive strain injury
- (B) Repetitive self-injury
- (C) Restrictive system injury
- (D) Repetitive strain injury

**7. The static shock one commonly feels is typically about how many volts?**

- (A) 3,000
- (B) 200

- (C) 10
- (D) 5

**8. You can prevent damage from ESD by**

- (A) Keeping the air dry
- (B) Using a multimeter
- (C) Using a grounding wrist strap
- (D) Using a TORX screwdriver

**9. Which of the following components would you use to help protect the computer from spikes in electrical power?**

- (A) Battery backup
- (B) Air filter
- (C) ESD wrist strap
- (D) Surge suppressor

## *Answers*

1. **B, C.** Examples of high-voltage equipment are CRTs and PSUs. *See “[Recognizing high-voltage equipment](#).”*
2. **B.** Computer chips and components can be killed with about 200V. *Review “[ESD means electrostatic discharge \(not extrasensory deprivation\)](#).”*
3. **D.** You should place computer components such as memory modules, cards, and hard drives in antistatic bags when storing those items and when transporting them from one location to another. *Check out “[ESD means electrostatic discharge \(not extrasensory deprivation\)](#).”*
4. **B.** Material Safety Data Sheet, or MSDS, is a document that shows the composition of hazardous materials and how to handle those materials. *Peruse “[Watching Out for EMI](#).”*

5. **B.** The Environmental Protection Agency (EPA) provides guidelines on how the components should be disposed of. *Take a look at ["Handling Toxic Waste."](#)*
6. **D.** When you continuously work with your computer for prolonged periods of time, there is a chance of developing a repetitive strain injury. *Peek at ["Exploring Ergonomics."](#)*
7. **A.** The shock we give one another is typically 3,000V. *Look over ["ESD means electrostatic discharge \(not extrasensory deprivation\)."](#)*
8. **C.** You can prevent damage from ESD by using a grounding wrist strap. *Study ["Component handling and preventing ESD."](#)*
9. **D.** Connecting the computer to a surge suppressor will prevent damage to a computer from a spike in power, or power surge. *Review ["Power-related issues."](#)*

# Chapter 4

## An Overview of System Components

---

### IN THIS CHAPTER

- » Introducing the basic components that make up personal computers
  - » Identifying the fundamental principles that apply to personal computers
- 

This chapter defines basic terminology and provides a brief overview of many topics that are covered in this book. By the time you finish reading this chapter, you should have a good understanding of the major components of the personal computer, from the motherboard to the monitor.

In preparation for the rest of the minibooks, I give you an overview of the major elements that make up the modern computer. As an A+ Certified Professional, you must be aware of these components, be able to service and manage these components, and be able to explain computing concepts to other people.

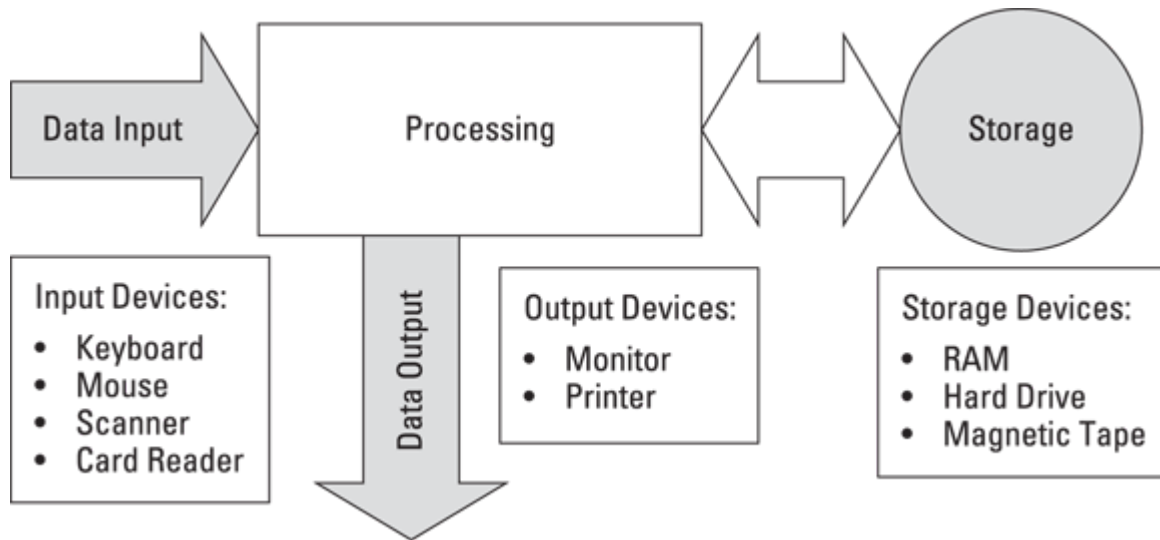
## *What Is a Computer?*

Computers are a major element of our society, and they exist in so many places that we tend to forget they are there. In simple terms, all computers are made up of four basic functions:

- » Data input
- » Data output
- » Processing

## » Storage

These functions, along with their related devices, are illustrated in [Figure 4-1](#). In this chapter, I briefly introduce each of these functions and devices, which are covered in depth in [Book 2](#), [Book 3](#), and [Book 8](#).



**FIGURE 4-1:** The major functions of the computer.

Although the packaging of these functions takes very different shapes, from smartphones and digital video recorders (DVRs) to routers, laptops, and tower computers, they all share these functions at the most basic layer. The CompTIA A+ certification exams focus on the common arrangement of devices performing these four functions — typically called the *personal computer* — and not the more obscure arrangement of devices (such as the automobile engine idle controller). The rest of this chapter guides you through the major components in the personal computer.

## *Looking Inside the Box*

Most of the processing and storage devices show up “inside the box.” This section gives you a look at the major elements that you will find inside the system housing, or case.

### *Processor/CPU*

The *processor* (also known as the central processing unit, or CPU) is the “brains of the organization,” so to speak. It is designed to do very few things, but to do them extremely quickly. The processor performs a limited set of calculations based on requests from the operating system and controls access to system memory. Processor speed is measured in several different ways, including clock cycles or megahertz (MHz) and gigahertz (GHz), and millions of instructions per second (MIPS). Any of these measures give you an estimate of the processor’s speed/power.

The speed of early processors ranged from 4 MHz to 8 MHz, but today’s processors have broken the multi-gigahertz (GHz) mark. With the advent of multiple core processors, the processor’s speed is usually represented as a “per core” value.



TIP

You can find processors covered in detail in Book 2, [Chapter 2](#).

## *Storage devices*

*Storage devices* on your computer are responsible for storing data, such as the operating system, applications, and actual output of applications or user data. Depending on the amount and type of data, the five basic types of devices to work with are

- » **Magnetic drives**, in various dimensions (such as 3.5 and 2.5 inches). These are typically referred to as hard disk drives (HDDs).
- » **Solid-state drives (SSDs)**, which are like hard drives. These drives are internal drives to store data, but unlike hard drives, these drives do not have moving parts, but rather use flash memory to store data. An SSD drive provides a substantial performance benefit.
- » **Hybrid drives**, which are standard hard drives with a small integrated SSD (4 to 16GB) that are used to cache data from the larger 1 to 4TB drive. These drives are designed to offer greater performance than standard hard drives for certain types of workloads. These drives would be most beneficial where most reads and writes occur with a small number of files, such as typical office tasks (word processing or

spreadsheets), but not very useful for tasks such as media production or hosting virtual machines.

- » **Optical drives**, including CD-ROM and DVD drives.
- » **Flash drives**, which store data in a variety of nonvolatile memory chips.

Any one of these formats enables your computer to store and retrieve data. Each of these storage options is considered to be long-term or permanent storage, but either descriptor is relative because each media format has a limited lifespan.

When dealing with storage devices, the four major technologies used to connect hard drives to motherboards are

- » **IDE** (Integrated Drive Electronics), **ATA** (Advanced Technology Attachment), or **PATA** (Parallel ATA) after the arrival of SATA.
- » **SATA** (Serial ATA)
- » **SCSI** (Small Computer System Interface)
- » **SAS** (Serial Attached SCSI)

An ATA controller allows the 40-pin IDE connector to accept a wide variety of devices while maintaining full backward-compatibility with traditional IDE drives or devices. In most cases, IDE and ATA are used interchangeably, while the current systems are technically using ATA technology. There has been a long, ongoing battle for speed and performance between IDE (or ATA) and SCSI; in general, SCSI provides faster and more reliable transportation, and IDE has been the low-cost alternative. SATA is IDE's younger cousin, and helps in IDE's fight to challenge the benefits of SCSI, which has had its support bolstered by SAS.



FOR THE  
EXAM

Do not forget that ATA and IDE terms are used interchangeably, but you do not want to confuse these terms with Serial ATA, which uses different technology, including signaling, transfer methods, and connectors.

Within a computer, a *bus* is a mechanism that is used to move data between devices of the computer, much like how a city bus is used to move people between bus stops in the city. Hard drives are manufactured as ATA, SATA, SCSI, or SAS devices, and they are usually connected to the motherboard through the high-speed PCI (Peripheral Component Interconnect) bus. However, being internal devices, they cannot be easily transported between computers. The USB and ThunderBolt buses provide fast-enough data transfer to allow hard drives to be attached to a system using these technologies, and are designed to be used with external devices. Many manufacturers have products that allow standard ATA or SATA drives to be connected using these buses. Because of the higher cost and the difference in technology, SCSI drives are not normally used.



TECHNICAL  
STUFF

Although SATA is usually thought of as an internal technology, there was been a rise in popularity of eSATA (External SATA), which provides an external connector to the SATA bus. Some external USB hard drives also support eSATA connectors. My last laptop even had a combination eSATA/USB connector. With the rise of USB3 and Thunderbolt, eSATA has dropped sharply in use.

The type of drives that you can attach to your computer depends on the types that are supported by your motherboard and I/O (input/output) cards.





TIP

You can investigate what you need to know about hard drives and storage devices for the A+ exams by going to Book 2, [Chapter 5](#).

## Memory

*Memory* is a *solid-state* (that is, no moving parts) storage medium. It can take many forms, such as RAM (random access memory), flash RAM, ROM (read-only memory), or EPROM (erasable programmable ROM). Access time for RAM is measured in *nanoseconds* (one-billionth of a second). When memory is discussed, it usually refers to RAM, which is the computer's primary working memory. RAM is a form of storage albeit typically temporary storage. Many people might not think of RAM as a storage medium because it is volatile and loses its information when power is removed, but temporary storage is still storage.



FOR THE  
EXAM

RAM is always temporary, and requires power to retain information. When you put your computer into a hibernation state, the contents of RAM are written to a file, and then retrieved when you power up your computer.

An analogy that I often use when talking about RAM is that of a tabletop (RAM) and a filing cabinet (hard drive or magnetic tape). People will not argue the point that a filing cabinet is a storage area for my papers, but they might dispute that a tabletop is a storage area. When I want to work with my papers, I take them out of the filing cabinet, and place them in temporary storage on my tabletop, where I am able to read the papers and make changes to them. When I am done, I will place the papers back in the permanent storage of the filing cabinet. I know some people who would use their tabletop as a form of permanent storage. Just like with RAM, my tabletop has a limited space, so when it becomes full, I will find that my work gets slower as I have to shuffle papers about. When the OS loads, it loads into RAM; when applications load, they load into RAM; when you

open documents, they load into RAM; and when you need to send output to your monitor, the output is loaded into RAM before it appears on your monitor.

In addition to working memory, RAM is used in many areas of your computer. In most situations, it is used for caching data or dedicated to specific subsystems. Most video cards will have dedicated RAM on the video card, and processors and hard drives have special high-speed RAM for caching.



FOR THE  
EXAM

RAM is where you work with your data and programs, while ROM and EPROM memory in your computer holds the operating code for your computer, which includes the Power-On Self Test (POST) routine and motherboard level processes. Do not confuse ROM operating code with your Operating System (OS), which is stored on the hard drive and runs in RAM.



TIP

To be able to answer all the memory questions on the A+ exams, read through Book 2, [Chapter 3](#).

## *System boards*

The term *system board* describes any number of circuit boards that make up the internals of your computer, but it is used most often to describe the motherboard. The *motherboard* is the main board in your computer that contains the BIOS chips, RAM, I/O ports, and CPU. This board maintains the electrical pathways that enable all other components to communicate with each other.

Some service manuals use the term *daughter board* to describe a secondary board that contains motherboard functions, such as disk or I/O control. A *daughter board* is a board that contains some of the chips that could have been put on the motherboard but were not — perhaps because

of space limitations or for other reasons. It is common to see them used in laptops and other mobile devices.



**TIP** Motherboard information required for the A+ exams can be perused in Book 2, [Chapter 1](#).

## *Power supply*

The *power supply* does exactly what its name suggests: It supplies power to the rest of the components in the computer. The power supply takes 120 or 240 volts (depending on the country you are in) of alternating current (AC) from your electrical outlet and converts it to 3.3 V, 5 V, and 12 V of direct current (DC). It contains a number of leads that supply different voltages for different types of devices (such as hard drives, PCIe expansion cards, and floppy drives — which you will not likely have a need for).



**TIP** Book 2, [Chapter 6](#) provides you with all the information you need to answer the power supply questions on the A+ exams.

## *Adapter cards*

*Adapter cards* allow you to adapt your computer to another role (such as controlling assembly line robots) or to add specific functionality to your computer (such as printing). The most common adapters are now integrated into most motherboards. These components include display, network, keyboard controller, mouse controller, serial ports, parallel ports, FireWire ports, and USB ports.

When the first computers came out on the market, most of the elements (if not all of them) were added to the motherboard by using the adapter slots, such as ISA, PCI, and PCI Express (well, ISA anyway, because the other slots did not exist).

## *Cooling system and fans*

As electricity moves through any circuit, heat is generated, which is illustrated by looking at a simple circuit that contains an incandescent light bulb. As electricity moves through the bulb, the filament heats to glowing. Heat is also generated while electricity moves through the integrated circuits that are contained in most of the components of the computer. In addition to these fixed integrated circuits, hard drives contain moving parts that generate heat from friction. These components generate a large amount of heat, which needs to be removed from the critical components to prevent them from failing early in their careers.

To remove heat from computer systems, there has been a steady increase in the use of fans, vents, and other heat-dissipation units. Heat sinks with fans are commonly placed on processors and critical chipsets. *Heat sinks* are made of heat-conductive metals (usually aluminum or copper), with a solid side in contact with the chip that they are protecting and thin fins on the other side, thus putting greater surface area with the air, which helps dissipate or transfer heat to the air. The use of a fan with the heat sink allows more cool air to flow through the fins. Case vents and fans bring cool air into the computer housing, and also vent and pull out hot air.

Faster processors produce more heat. As processors have become faster, more methods for pulling the heat away from the processor have been developed, such as liquid-cooling systems.



**TIP** You will find answers to A+ exam questions related to cooling processors in Book 2, [Chapter 2](#); and for overall systems in Book 4, [Chapter 1](#).

## *Firmware and chipsets*

People like to keep their world in a perceived state of order to give themselves a sense of control. This is often seen by how we classify everything we see or work with into categories. Many of these categories seem very distinct until something comes along to challenge our opinions, and then the waters become murky.

One of these murky areas is the distinction between hardware and software, which at one point were thought to be distinct and separate. *Software* is programming code that is stored on your disk or on some other form of media. *Hardware* refers to the physical components — boards, peripherals, and other equipment — that make up your computer.

Firmware fills in a middle ground between software and hardware, where the distinct line begins to disappear. *Firmware* is programming code (software) that is contained in or stored on the IC (integrated circuit) chips (hardware) on your computer. This combination of hardware and software makes up the BIOS on several different devices, with settings stored in CMOS or flash RAM. This firmware is tied to the function of the IC chips that it is working with; in the case of a network card, firmware would manage network or PXE (Preboot eXecution Environment) boot functionality of the card.

Most modern motherboards have a series of IC chips and firmware that work together to control the integrated functions of the motherboard. The compatibility of these chips and the code that ties them together is provided by a single supplier, and this group of chips is referred to as a *chipset*. Intel and VIA Technologies produce popular chipsets.

## ***BIOS***

*BIOS* is short for *basic input-output system*. The BIOS is actually software that is stored on a ROM chip on the motherboard. Most systems today use a flash EPROM to store the BIOS so that the user can update the programming code in the BIOS.

The BIOS is responsible for controlling or managing low-level but extremely important processes like the *POST* (*Power-on Self-Test*), the boot process, and the interaction of components on the motherboard.

## ***UEFI***

*UEFI* stands for Unified Extensible Firmware Interface and represents the next generation of the low-level ROM-based code that controls motherboard processes, but with a great deal of enhancements. UEFI is capable of supporting advanced diagnostic tools, even without having an

OS installed on the computer. UEFI supports network booting, secure boot, and even has a limited shell for running commands.

To support BIOS-style system calls to load legacy operating systems, UEFI supports a legacy mode.



**TIP**

Book 2, [Chapter 4](#) provides you with all the facts that you will need to answer BIOS and UEFI questions on the A+ exams.

## **CMOS**

*CMOS* (complementary metal-oxide semiconductor) is often confused with BIOS/UEFI. BIOS/UEFI is programing code that is stored on a ROM and EPROM chip and controls the loading of the operating system as well as low-level functions. BIOS/UEFI often has settings that the user may control, and these settings are stored in CMOS memory, where CMOS refers to the type of manufacturing process that creates this integrated circuit and most other integrated circuits.

Most RAM chips rely on CMOS technology to store information, but when discussing CMOS, you will be referring to the hardware configuration settings that are saved between reboots of your computer. Because these settings are stored in RAM, they require power to maintain the information, and in the case of CMOS, the power is usually supplied by a small battery on the motherboard. These settings include

- » Which hard drives and floppy drives are present
- » How much memory is installed
- » Whether booting requires a keyboard
- » The type of mouse installed (USB, PS/2, or serial)
- » What are the reserved resources (such as IRQ [interrupt request], I/O addresses, and DMA [direct memory access] channels)
- » What is the power-on password and whether it is required to boot up the system

- » The date and time
- » Whether ACPI (Advance Configuration Power Interface) is enabled and what devices it applies to



FOR THE  
EXAM

To be ready for your A+ exams, review the CMOS information, such as common settings, in Book 2, [Chapter 4](#).



FOR THE  
EXAM

Remember that BIOS/UEFI stores programming code, and CMOS stores settings for the BIOS/UEFI options.

## *Checking Outside the Box*

Now that you have looked at what is inside the box, you will want to see what gets added to the system — *outside* the box.

### *Cases and form factors*

Part of the outside of the box is the box itself. There are many different form factors for the box, some of which dictate the form factor of the motherboard going into the case. Computer cases are most often tower or desktop form factors, but are also found in sizes and shapes that make them attractive for entertainment units and in extremely small forms for specific uses.

The term *form factor* refers to the size of the object (be it hard drive, motherboard, or case), and many objects have industry specifications that define acceptable or allowed sizes. Motherboards and hard drives have industry-wide specifications, yet computer cases do not have specifications on their size or shape. Computer cases do need to adhere to the specifications of the internal components (such as hard drives and motherboards) to allow for these devices to be properly mounted inside of the case.

## *Input and output devices*

Computers use many different kinds of input and output devices (also called I/O devices), which connect to the computer via one of the computer's ports. In the following sections, I give you an overview of the most common input and output devices.

### *Monitor*

The different types of buses that can provide video services include

- » **PCI (Peripheral Component Interconnect)**, which runs at 33 MHz and 66 MHz and carries 32 bits of data (approximately 132 MBps or 264 MBps).
- » **PCIe (Peripheral Component Interconnect Express)**, or PCI Express, is a high-speed serial bus, so its speed is measured differently than the others, which are parallel buses.

PCIe has between 1 and 16 channels (1x–16x). Depending on the version (version 1.x, 2.x, or 3.0), PCIe can carry data at 250 MBps, 500 MBps, or 1 GBps, per channel, per direction. ISA and PCI are half duplex — data can only flow in one direction at a time, while PCIe is full duplex — data may flow in both directions simultaneously. For a 16-channel card, the speeds for the three versions would be 4 GBps, 8 GBps, or 16 GBps.



**TIP** PCIe is a newer, faster bus that is widely used on servers, desktops, and laptops alike. Laptops do make use of a smaller format PCIe connector in the form of MiniPCI Express.

You have probably already guessed that the faster the bus speed, the faster your video card is likely to function. In addition to a fast bus speed, video performance and color depth are provided by RAM or video RAM. This RAM is found on the video card itself. Some high-end video cards also have a small processor (graphics processing unit or GPU) to handle some of the work of displaying information on your monitor instead of letting the computer's main processor do all the work.





TECHNICAL  
STUFF

The processing done by some video cards can require that the card receive additional power from the power supply, rather than relying solely on the power provided by the bus. This is why some power supplies have a special 12VDC connector for your video card.

Video cards traditionally have a limit on how many colors they support, which is called color depth, and include

- » 4-bit or 16 colors
- » 8-bit or 256 colors
- » 16-bit or 65,000 colors
- » 24-bit or 16 million colors
- » 32-bit or 4 billion colors

Standard screen resolutions for the 4:3 aspect ratio are (in pixels)

- » 640 x 480
- » 800 x 600
- » 1024 x 768
- » 1152 x 864
- » 1280 x 1024
- » 1600 x 1200
- » 1920 x 1440

With the prevalence of wide-screen monitors (16:10 aspect ratio), standard wide-screen resolutions (or dimensions) are (in pixels)

- » 768 x 480
- » 1024 x 640

- » 1152 x 720
- » 1280 x 800
- » 1680 x 1050
- » 1920 x 1200
- » 2560 x 1440

The new kid on the video block is 4K video, providing a standard that goes up to 4096 x 2160 with an aspect ratio of 1.90:1. While video standards continue to evolve and support higher resolutions with each passing year, modern monitors and video cards support a minimum level of support that follows the SVGA (Super Video Graphics Array) standard of 256 colors at 800 x 600. This is only included for backward compatibility with older devices and replaces the previous fallback level of support, which was VGA. The VGA standard is output in 16 colors at 640 x 480. You can expect to see this fallback level increase to the XGA (Extended Graphics Array) in the future, which supports 256 colors at 1024 x 768.



**TIP** Review Book 3, [Chapter 3](#) to fully understand monitors and video.

## ***Ports***

Sailing ports provide a location for ships to load and unload goods from one location to another. On your computer, *ports* act as connection points for cables, which allow for the transfer of data between your computer and another device. Several different types of connectors and cables are used to join devices. Although the list of devices that communicate through the different types of ports is limitless, some of the basic types of ports and their uses are listed in [Table 4-1](#).

**TABLE 4-1 Basic Types of Ports**

<i>Port</i>	<i>Use</i>
-------------	------------

<b>Port</b>	<b>Use</b>
Serial	Connects serial devices, such as modems, to your computer.
Video	Connects a monitor to your computer.
USB	Connects various types of devices to your computer. Devices that used other ports in the past are increasingly being converted to use USB ports. Devices that use this port include printers, modems, mice, keyboards, and scanners.
Keyboard	Connects a keyboard to your computer.
Mouse	Connects a mouse to your computer.



**TIP**

Reading through Book 3, [Chapter 1](#) will give you a full appreciation of all of the types of ports, cables, and connectors that are used by computers.

## *Getting an A+*

This chapter provides an overview of the major components found in a computer system, including

- » **System boards**, which contain most of the computer circuitry
- » **Power supply**, which converts a building's AC to usable DC for the computer
- » **Processor/CPU**, which efficiently executes instructions for the OS
- » **Memory**, which holds working data and application code
- » **Storage devices**, which are long-term or short-term storage areas
- » **Monitor**, which displays data from the computer
- » **Modem**, which communicates with other devices
- » **Firmware**, which is a cross-breed between hardware and software
- » **BIOS**, which are low-level internal communication routines
- » **CMOS**, which is a storage area for configuration settings

» **Ports**, which are used as connection points for other devices

## *Prep Test*

- 1. Which of the following components is not usually found on a motherboard?**
  - (A) BIOS chips
  - (B) USB drives
  - (C) Memory
  - (D) I/O ports
  
- 2. What type of memory loses its contents when power is turned off on your computer?**
  - (A) CMOS memory
  - (B) RAM
  - (C) ROM
  - (D) EPROM
  
- 3. A standard power supply converts 120V AC or 240V AC to which of the following? (Select all that apply.)**
  - (A) 3.5 V DC
  - (B) 3.3 V DC
  - (C) 6 V DC
  - (D) 12 V DC
  
- 4. What is the primary purpose of the processor?**
  - (A) To convert digital signals into analog signals
  - (B) To process signals so that they can be displayed on your monitor
  - (C) To carry out instructions from the operating system
  - (D) To convert 16-bit data into 8- or 32-bit data

**5. What unit is used to measure RAM speed?**

- (A) Milliseconds
- (B) Gigaseconds
- (C) Picoseconds
- (D) Nanoseconds

**6. Which two of the following represent hard drive architectures?**

- (A) PCI
- (B) IDE
- (C) CMOS
- (D) SCSI

**7. What is the standard most current monitors support for fallback when using older video cards?**

- (A) VGA
- (B) SVGA
- (C) CGA
- (D) PAL

**8. Firmware is composed of which of the following? (Choose two.)**

- (A) Software
- (B) Middleware
- (C) Hardware
- (D) CMOS

**9. The programs that allow the POST to take place are stored in what?**

- (A) BIOS
- (B) CMOS
- (C) RAM
- (D) POSTOS

**10. What does CPU stand for?**

- (A) Core predetermination utility
- (B) Complementary provider unit
- (C) Central processing unit
- (D) Co-primary uniprocessor

**11. What does CMOS stand for?**

- (A) Complementary metal-oxide semiconductor
- (B) Co-management of operating system
- (C) Configuration management and option semiconductor
- (D) Configuration memory option system

## *Answers*

1. **B.** The motherboard will include I/O ports or connectors for a variety of devices, but will not typically include the devices themselves. It will include the ATA controller and also a connector to attach the ATA drive, but not the drive itself. The same would be true of USB drives; the motherboard will include the controller and connector for the USB bus but not the actual device. See “[System boards](#).”
2. **B.** RAM memory is *volatile*, or non-permanent, because it loses its contents when power is turned off on the computer. Review “[Memory](#).”
3. **B, D.** Power supplies have leads that supply 3.3 V, 5 V, or 12 V. Check out “[Power supply](#).”
4. **C.** Processors carry out instructions that they receive from the operating system. Peruse “[Processor/CPU](#).”
5. **D.** The normal measurement for RAM is nanoseconds, or billionths of a second. Take a look at “[Memory](#).”
6. **B, D.** Hard drive architectures used with computers are IDE (or ATA), Serial ATA (SATA), SCSI, and Serial Attached SCSI (SAS).

Peek at “[Storage devices.](#)”

7. **B.** Super Video Graphics Array (SVGA) is the current graphics standard that monitors follow. *Look over “[Monitor.](#)”*
8. **A, C.** Firmware consists of programming code or software that is contained within a hardware component such as a ROM chip. *Refer to “[Firmware and chipsets.](#)”*
9. **A.** BIOS contains the programs that allow the POST to take place. The BIOS is stored on a ROM or an EPROM. *See “[BIOS.](#)”*
10. **C.** Central processing unit. *Review “[Processor/CPU.](#)”*
11. **A.** Complementary metal-oxide semiconductor. *Check out “[CMOS.](#)”*

# Book 2

## Inside the Box

### Contents at a Glance

#### Chapter 1: Knowing Your Motherboard

[What's on the Front Panel](#)  
[Finding Out What's on a Motherboard](#)  
[Identifying the Types of Motherboards](#)  
[Understanding Bus Architectures](#)  
[Performance Considerations](#)  
[Getting an A+](#)  
[Prep Test](#)  
[Answers](#)

#### Chapter 2: Picking Your Processor

[Understanding Processor Terminology](#)  
[Identifying Socket Types](#)  
[Looking at Intel Processors](#)  
[Don't Forget Non-Intel Chips](#)  
[Installing a Processor](#)  
[Keeping a Processor Cool](#)  
[Increasing Performance](#)  
[Getting an A+](#)  
[Prep Test](#)  
[Answers](#)

#### Chapter 3: What to Remember about Memory

[Understanding the Types of Memory](#)  
[Identifying the Types of DRAM](#)  
[How Would You Like Your Chips Packaged?](#)  
[Understanding Error-Checking Memory](#)



[Multichannel Memory Architecture](#)  
[Single-Sided versus Double-Sided Memory](#)  
[Buffered versus Unbuffered Memory](#)  
[Working with Cache Memory](#)  
[Installing or Upgrading Memory](#)  
[Getting an A+](#)  
[Prep Test](#)  
[Answers](#)

## **Chapter 4: Telling Your BIOS from Your CMOS**

[BIOS versus CMOS](#)  
[Upgrading the System BIOS/UEFI](#)  
[Understanding CMOS](#)  
[Viewing Basic Interface Settings](#)  
[Viewing Advanced CMOS Settings](#)  
[Getting an A+](#)  
[Prep Test](#)  
[Answers](#)

## **Chapter 5: Working with Storage**

[Understanding Hard Drive Terminology](#)  
[Discovering IDE Devices](#)  
[Learning How SCSI Works](#)  
[Understanding Serial ATA](#)  
[A Quick Tour of RAID](#)  
[Using Removable Storage](#)  
[Troubleshooting Hard Drives and RAID Arrays](#)  
[Getting an A+](#)  
[Prep Test](#)  
[Answers](#)

## **Chapter 6: Working with Power**

[Knowing the Basics of Power Terminology](#)  
[Identifying the Purpose of Power Supply Units](#)  
[Identifying Power Supplies](#)

[Power Connectors](#)

[Power Supply Form Factors](#)

[Using AC Adapters](#)

[Working with UPS and Suppressors](#)

[Getting an A+](#)

[Prep Test](#)

[Answers](#)

# Chapter 1

## Knowing Your Motherboard

---

### IN THIS CHAPTER

- » Distinguishing motherboard components
  - » Recognizing types of motherboards
  - » Identifying bus architectures
- 

One of the major replaceable components in your computer is the *system board*, also known as the motherboard. The *motherboard* is the big green board (that might not be a technical description, but I think that looking inside your system will demonstrate that it is an accurate one) connected to the computer case. It is the motherboard that holds your RAM, processor, and a number of other components in place.

Think of the motherboard as the glue that connects all the other PC components. For example, you can see how the hard drive is connected to the motherboard by following the SATA cable from your hard drive to the motherboard. The memory sockets and the processor socket are likewise located on the motherboard.

In short, all the components that work together to make the computer functional connect to the motherboard. If you take a close look at the motherboard, you can see wires embedded on the board that form little pathways that span the system. Think of these wires as the highway system that data signals use to travel from one location to another.

In this chapter, I introduce you to the different types of components found on the motherboard. After identifying the motherboard components, you find out about the different types of motherboards. Finally, you explore what an expansion bus is and discover the different bus architectures.

# *What's on the Front Panel*

Before looking at the internals of the computer and identifying the motherboard components, I'll first look at what is on the outside of the computer. The buttons and lights that are found on the outside of the computer can help you identify what is going on with the computer itself. For example, if you notice that the system is not responding but you see that the hard drive light is flashing, you know that the system is not responding because it is busy.

The front panel of the computer will vary from system to system, but most systems may have the following elements:

- » **USB:** On the front panel of most systems you will notice a few USB ports that are used to connect USB devices such as flash drives, external drives, or digital cameras to the system.
- » **Audio:** The front panel usually contains an audio port to connect headphones to the system and maybe a Line In port as well to connect other audio sources to the computer.
- » **Power button:** The Power button is usually found on the front panel so that you can power the system on. If the system freezes up on you, you may have to power off the system and then on with a *cold boot*. A *cold boot* is when you shut off the power and then power it back on by using the Power button.
- » **Power light:** You usually find a power light on the front of the system so that you can tell whether the system is running.
- » **Drive activity light:** The drive activity light will flash when the system is busy.
- » **Reset button:** Some systems come with a Reset button, which is used to do a *warm boot* of the computer. A *warm boot* is a reboot without cutting the power to the system, but the system still shuts down and restarts.

# *Finding Out What's on a Motherboard*

When you look at the motherboard inside your computer, you notice that a number of different items connect to it. The memory sockets, CPU socket, and BIOS chip are all located on the motherboard. In this section, I identify the different components that are interconnected via the motherboard.

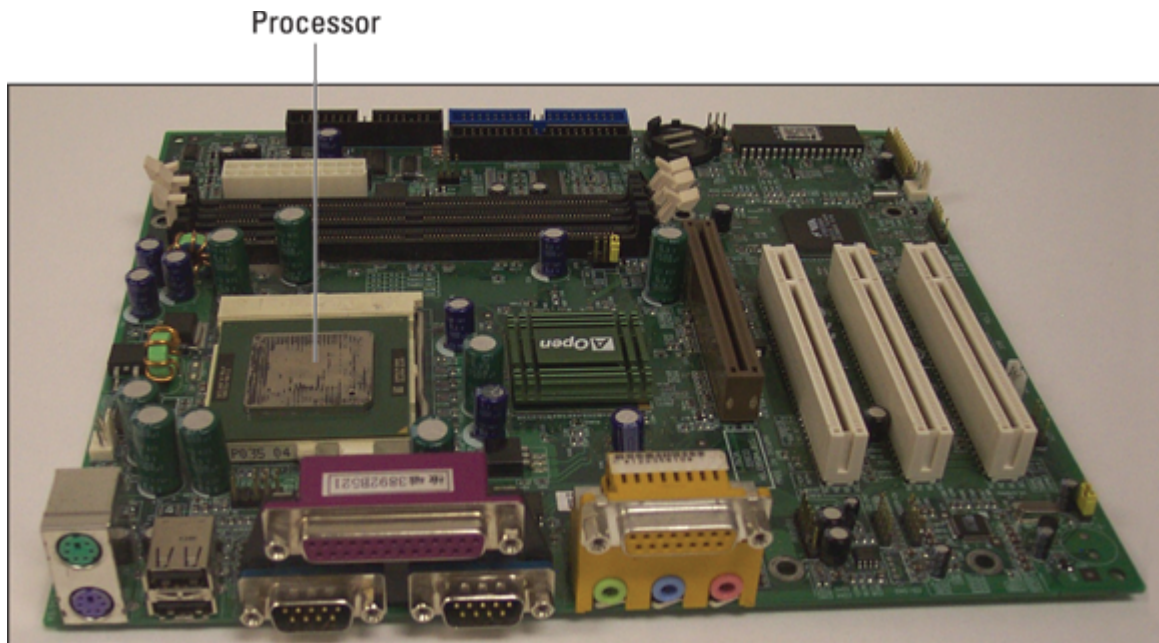


FOR THE  
EXAM

The terms *system board* and *motherboard* are interchangeable.

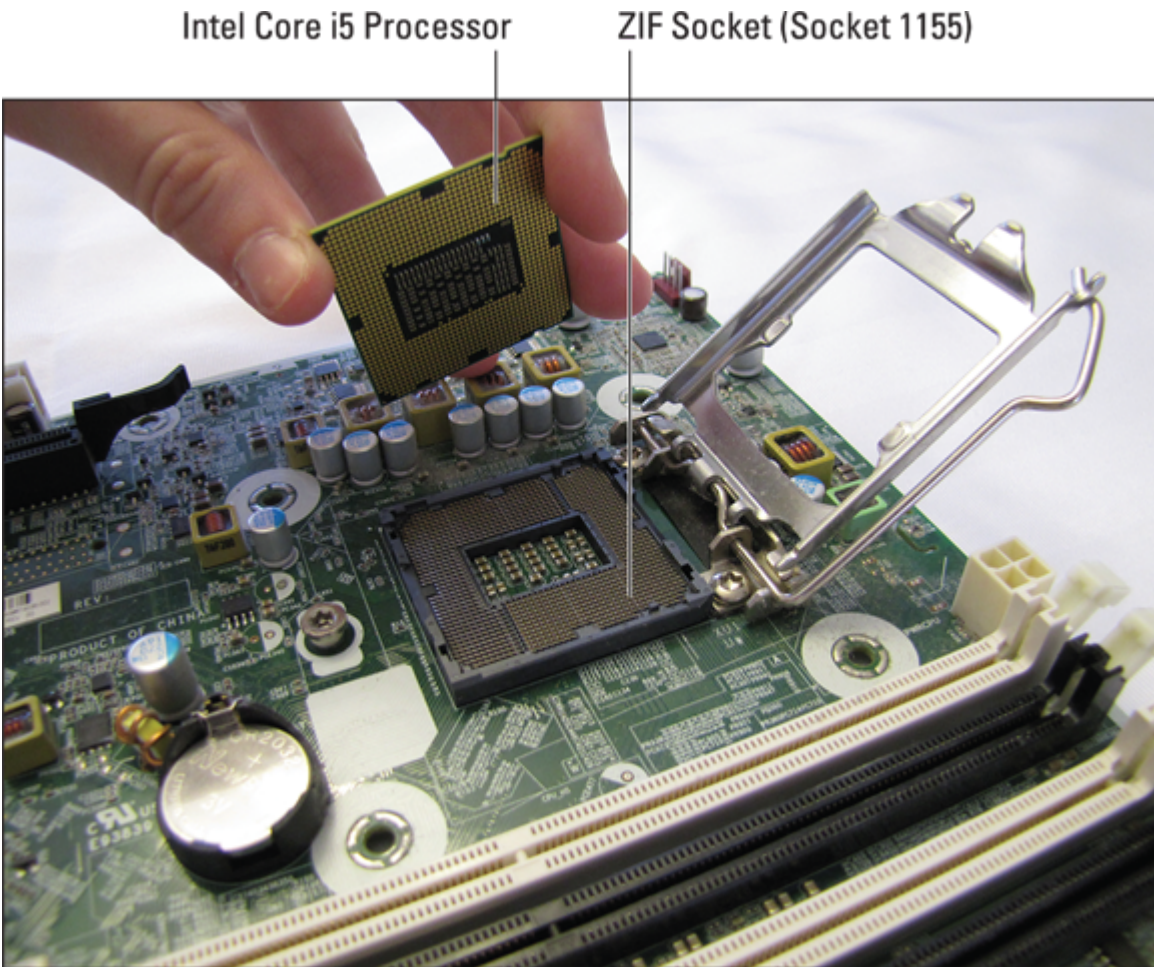
## *Processor/CPU sockets*

One of the easiest items to identify on the motherboard is the *processor*, also known as the *central processing unit* (CPU). The processor is usually the largest chip on the motherboard and is one of the few chips with a heat sink or a fan on top of it, as shown in [Figure 1-1](#).



**FIGURE 1-1:** A processor on a motherboard.

The motherboard has a socket that the processor is inserted into. Today, this socket is implemented as a *zero insertion force (ZIF)* socket, which means that the processor chip can be removed or added to the socket with very little effort. ZIF sockets (shown in [Figure 1-2](#)) typically have a lever that you pull to pop the processor out of the socket.



**FIGURE 1-2:** A ZIF socket on the motherboard.



**FOR THE  
EXAM**

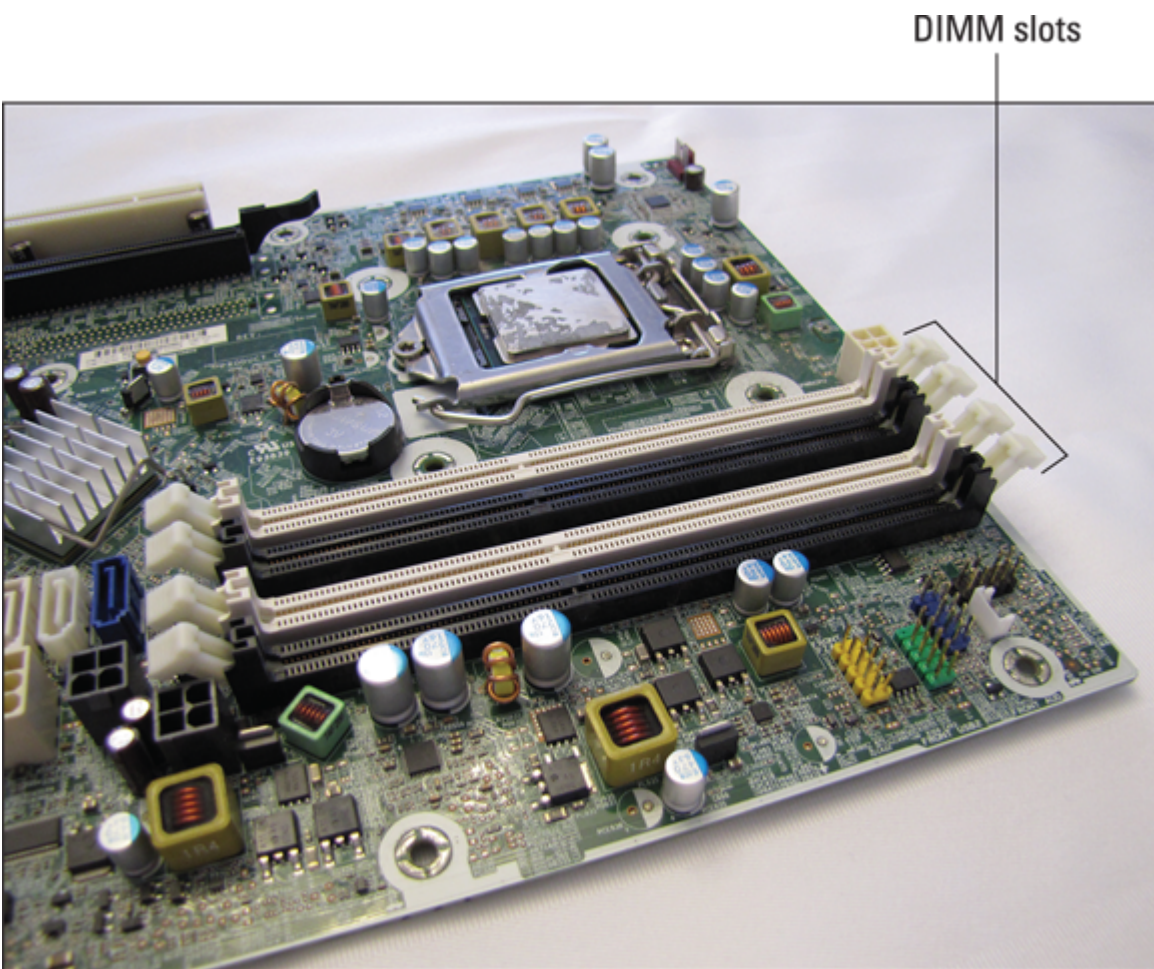
Remember that the Pentium 4 is placed in Socket 423 or Socket 478, while the Intel Core i5 is placed in sockets 1155, 1156, and 1150. Intel Core i7 is placed in socket 1366 and socket 1156.

## *RAM slots*



When you look at a motherboard, one of the first items that should stand out is the processor; the next things you will usually notice are the memory slots used to install RAM into the system.

You should be familiar with the types of sockets for installing memory for the A+ certification exams: *dual inline memory module (DIMM)* sockets. System boards today will have a number of DIMM sockets to install memory. There are no rules as to how many DIMM sockets a motherboard manufacturer may use. [Figure 1-3](#) shows a motherboard with four DIMM sockets used to hold DIMMs.



**FIGURE 1-3:** DIMM memory slots on a motherboard.

You can install DIMMs individually or you can install them in a dual-channel architecture by filling the black slots or the blue slots (and sometimes the slots are white, as shown in [Figure 1-3](#)) with the same size

and speed memory module. Dual-channel architecture increases performance by being able to send and receive data in two 64-bit chunks as opposed to one 64-bit chunk, as is the case with normal memory configurations.

DIMMs are 64-bit memory modules — the same number of bits as the data path of the CPU — which is why you can install them singly if you wanted to. (The reason I mention this is because back in the original Pentium days we had memory modules known as Single Inline-Memory Modules [SIMMs], which were 32-bit modules that you had to install in pairs. Keep in mind that you do not need to know SIMMs for the new A+ certification exams!) For more information on memory banks and installing memory, check out Book 2, [Chapter 3](#).

## *Cache memory*

*Cache memory* increases performance by storing frequently used program code or data that can be later accessed by the processor. Cache memory is much faster memory than normal RAM and, as a result, is more expensive. The system stores data accessed from RAM in cache memory when the data is accessed the first time, making subsequent requests to the same data faster because the data is accessed from cache (faster than RAM) for subsequent calls.

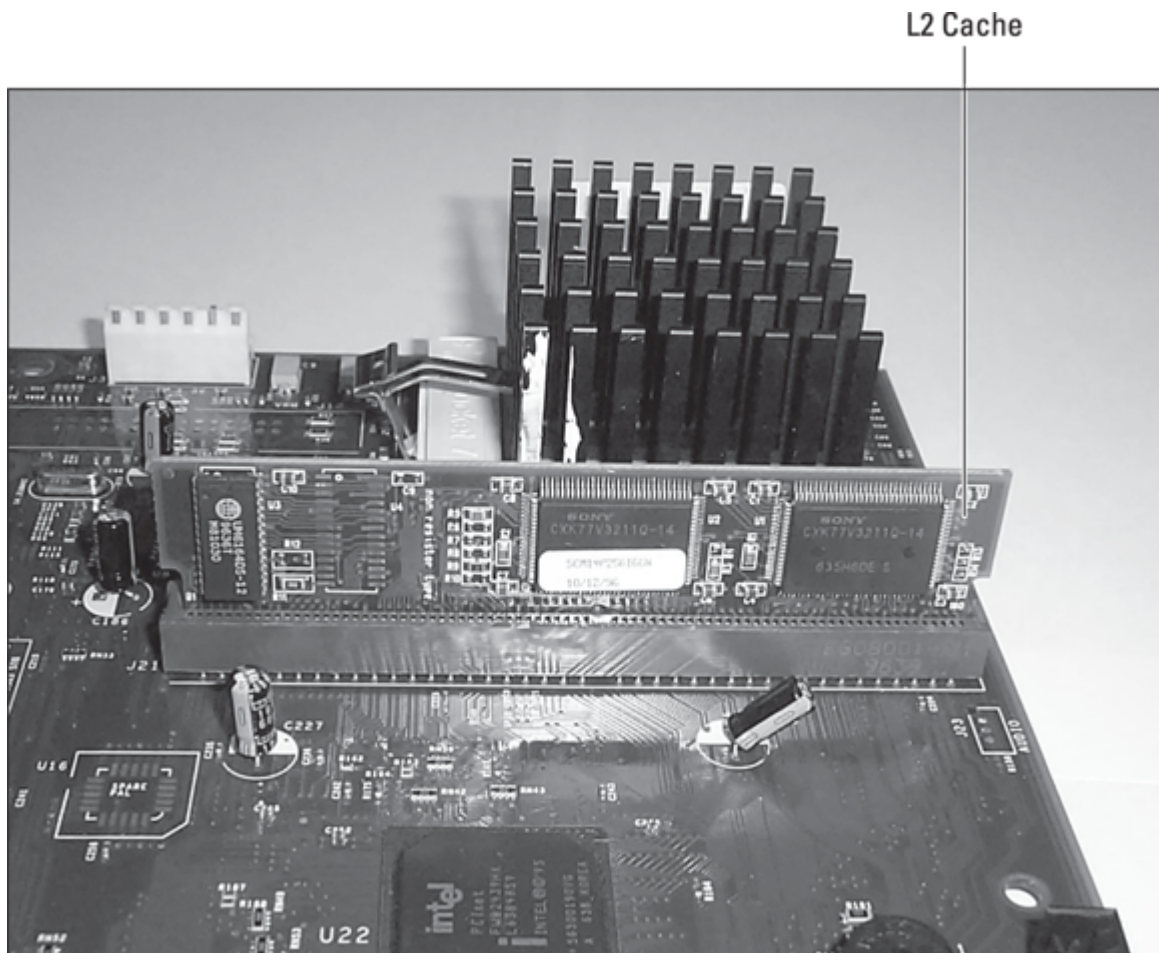
All processors today have integrated cache memory, which is known as *level 1 cache*. *Integrated cache* is cache memory that is built into the processor, while *nonintegrated cache* — known as *external cache* — is built outside the processor, typically on the motherboard. The types of cache are as follows:

- » **L1 (level 1) cache:** Cache integrated within the processor.
- » **L2 (level 2) cache:** Many years ago, L2 cache was cache memory that you added to the motherboard, but nowadays, processors ship with amounts of L2 cache independent for each processor core.
- » **L3 (level 3) cache:** Level 3 cache is cache memory that ships with the processor that is shared between each processor core.



Many years ago, older motherboards implemented cache memory as rows of DIP (dual inline package) chips placed directly on the motherboard. This area was sometimes even labeled “cache.” Unfortunately, you can’t expect a motherboard to be well labeled; if you find labels (in English), consider it an added bonus! For more information on chip packages, check out Book 2, [Chapter 2](#).

Other systems have implemented the cache as a memory module, so you might see an empty slot on the motherboard that looks like a DIMM slot but will really hold a cache module. A lot of times, this is labeled as “cache” on the motherboard. [Figure 1-4](#) shows L2 cache on an older motherboard.



**FIGURE 1-4:** L2 cache located on an older motherboard.



FOR THE  
EXAM

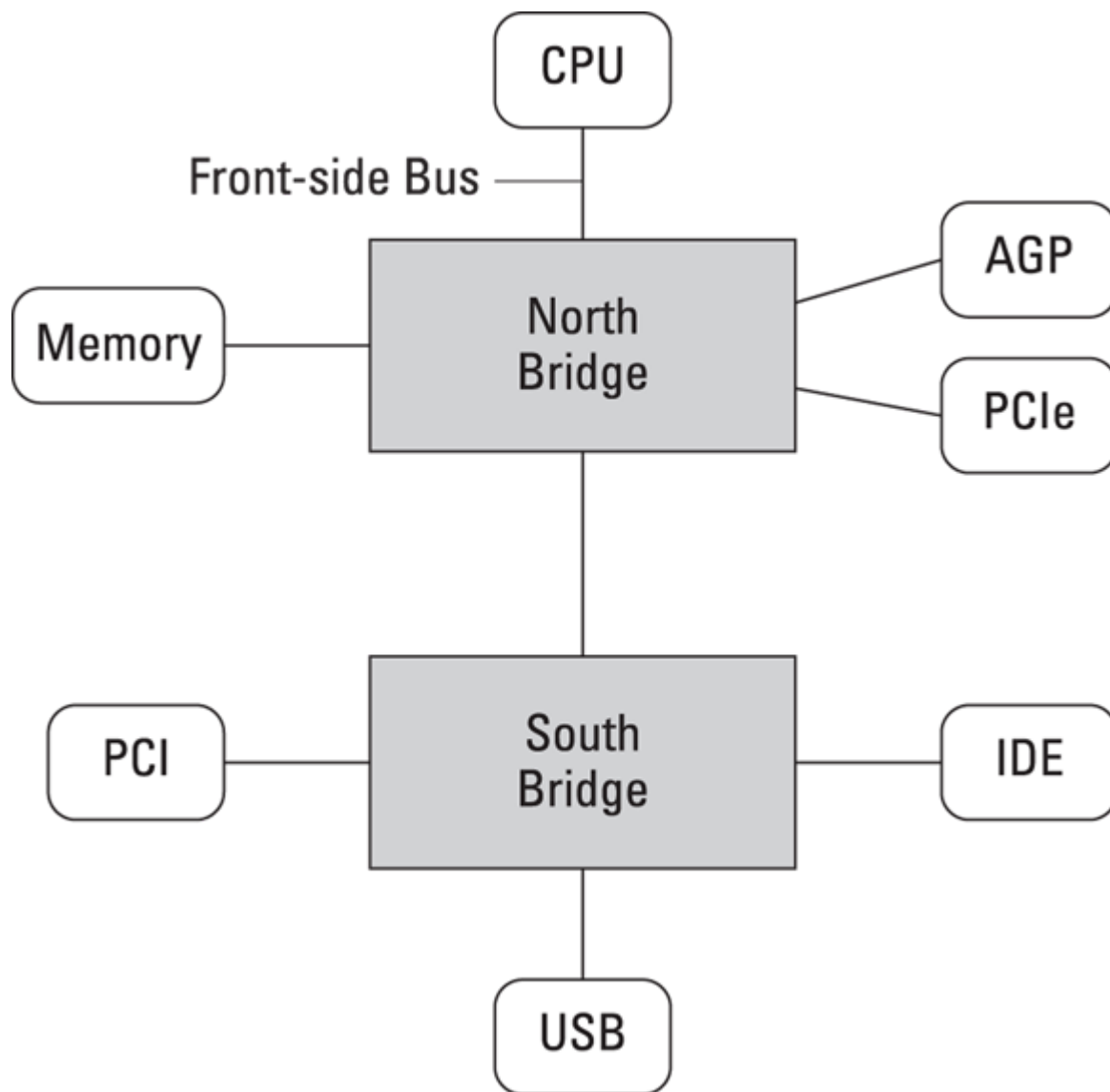
L2 cache is usually located on the motherboard near the processor. That way, data travels over a shorter distance from cache to processor, thus increasing overall system performance. Also note that today's processors implement L1, L2, and L3 cache in the casing (known as the die) of the processor. For more information on cache memory, refer to Book 2, [Chapter 3](#).

## ***Motherboard chipset***

Each hardware component in the system has circuitry responsible for managing a specific hardware part. This circuitry is the *controller* for that specific piece of hardware. For example, access to memory is controlled by the *memory controller*, the hard disk is managed by the *hard disk controller*, and the keyboard is managed by the *keyboard controller*.

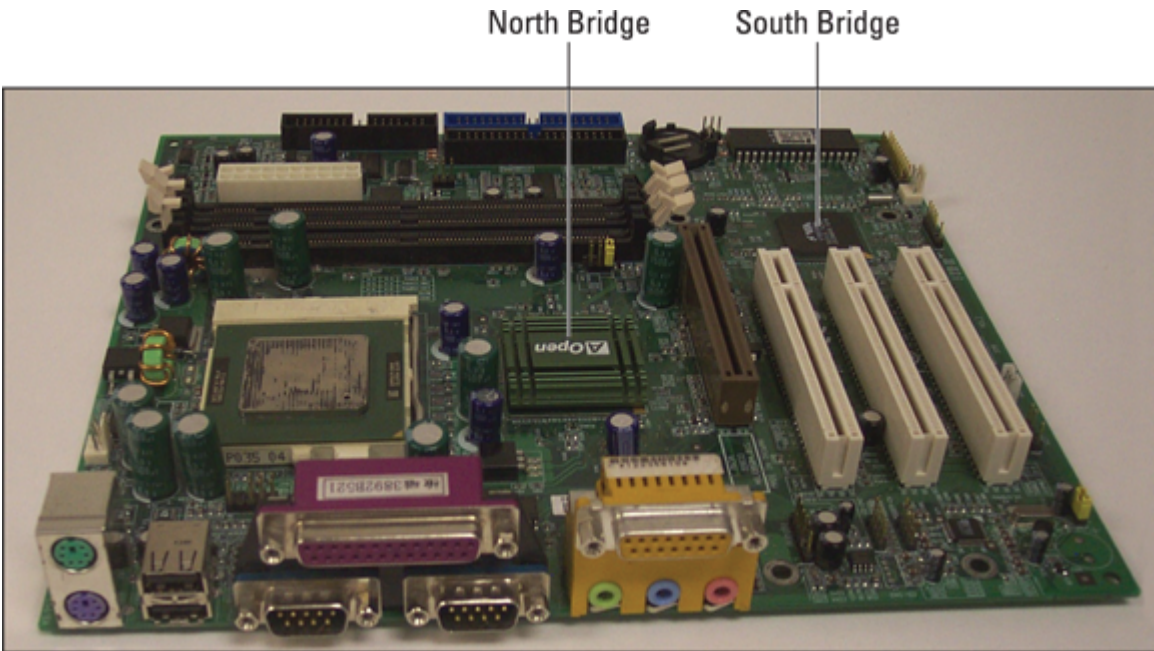
The combination of computer chips that hold the logic for these controllers is the *motherboard chipset*. Together, the computer chips make up the chipset control communication from the CPU to each of the hardware devices in the system.

Two chips that make up a big part of a motherboard's chipset are the North Bridge and the South Bridge. The *North Bridge* chip is responsible for communication from the CPU to memory, the CPU to the PCI Express bus (more on PCI Express later in this chapter), and the Advanced Graphics Port (AGP) device (more on AGP later in this chapter). The *South Bridge* chip is responsible for communication between the CPU and other devices, such as PCI, USB, ISA, and IDE devices. These two chips contain the bulk of the logic that allows a CPU to communicate with other hardware. [Figure 1-5](#) displays the relationship between the processor and the North Bridge and South Bridge chips.



**FIGURE 1-5:** The relationship between the CPU and the motherboard chipset.

Locating the North Bridge and South Bridge chips on a motherboard can sometimes be challenging. The North Bridge chip is typically the second largest chip (after the processor) and also typically contains a heat sink or a fan on top of the chip to keep it cool. The North Bridge chip is typically located around the processor, and on older motherboards it is found between the processor and the AGP slot. The South Bridge is normally located farther from the processor — usually beside the PCI slots, as shown in [Figure 1-6](#). Notice in the figure that the North Bridge chip bears the manufacturer name “AOpen” on it, and the South Bridge is the chip above the PCI slots.



**FIGURE 1-6:** The North Bridge and South Bridge chips on an AOpen motherboard.



**FOR THE  
EXAM**

Be familiar with the function of the North Bridge and South Bridge chips on the motherboard:

- » The *North Bridge* chip handles communication to high-speed buses such as memory, AGP, and PCI Express.
- » The *South Bridge* chip handles communication to all other motherboard components such as USB, PCI, IDE, and legacy hardware, including ISA devices.

You may find it difficult to locate the North Bridge and South Bridge chips on some motherboards today as the North Bridge has been moved into the CPU, while the South Bridge has been replaced by the Platform Controller Hub (PCH). The PCH is an Intel chipset that provides similar functionality to South Bridge so manufacturers removed the South Bridge and stuck it with the PCH chip.

## ***BIOS chip***

The *basic input-output system* (BIOS) is the low-level program code that allows all the system devices to communicate with one another. This low-level program code is stored in the BIOS chip on the motherboard.

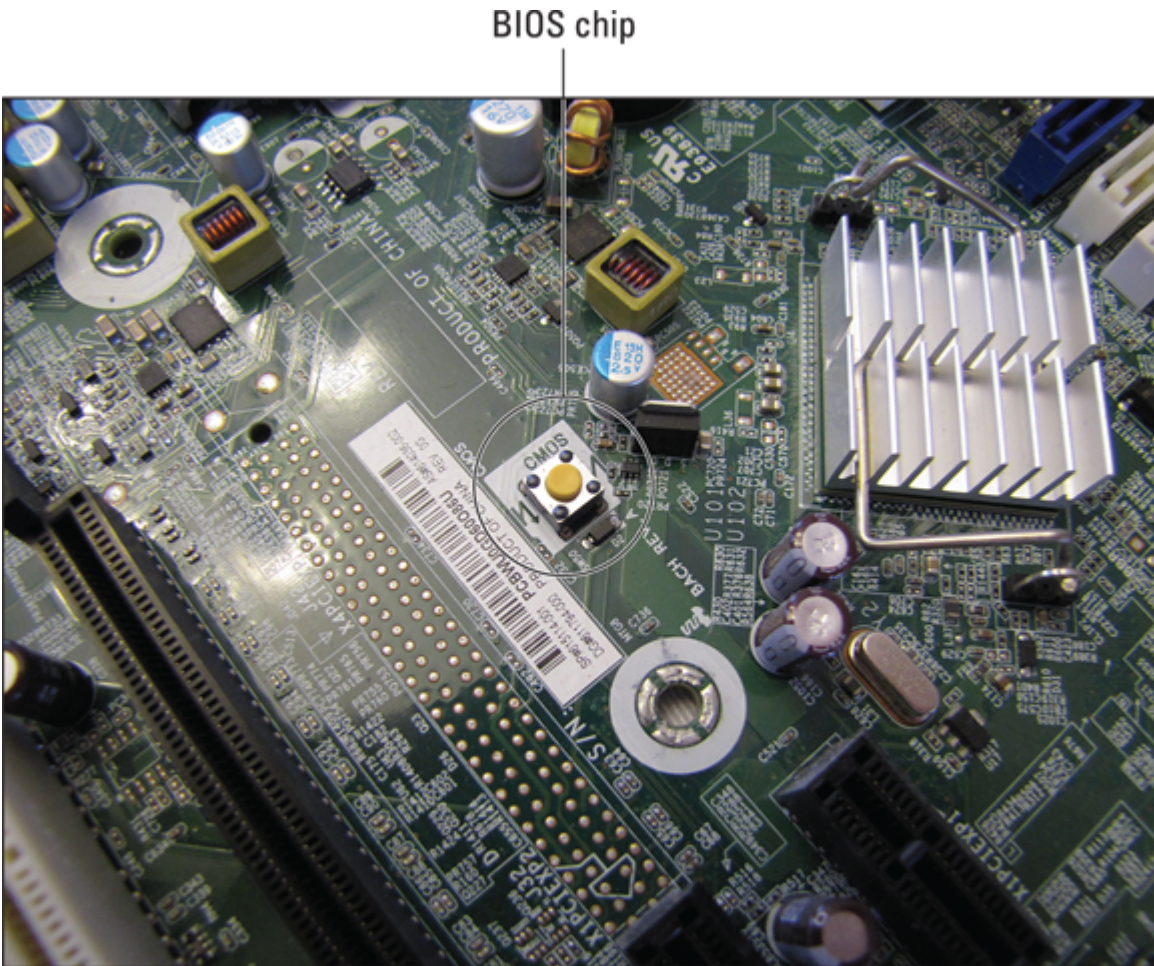
Locating the BIOS chip on older motherboards was easy; it was usually rectangular and generally features a label with the manufacturer's name and the year the chip was manufactured. Some of the popular manufacturers are AMI, AWARD, and Phoenix. Today's BIOS chips are usually much smaller chips and may not have a label on them. Instead you may find the motherboard is labeled (not the BIOS chip itself).

The BIOS chip is a *read-only memory* (ROM) chip, which means that you can read information from the chip, but you can't write to the chip under normal circumstances. Today's implementations of BIOS chips are *EEPROM* (*electrically erasable programmable ROM*), which means that you can get special software from the manufacturer of the BIOS to write to the chip.

Why would you want to erase the BIOS? Suppose, for example, that your BIOS is programmed to support a hard disk up to 200GB in size, but that you want to install a new, larger hard disk instead. What can you do about it? You can contact the BIOS manufacturer and get an update for your BIOS chip, which is usually a software program. (In the past, you generally had to install a new chip.) Running the software program writes new instructions to the BIOS to make it aware that there are hard disks bigger than 200GB and provides instructions for dealing with them. But before new instructions can be written, the old instructions need to be erased.

The BIOS chip also contains code that controls the boot process for your system. It contains code that will perform a *Power-on Self-Test* (POST), which means that the computer goes through a number of tests, checking itself out and making sure that it is okay. After it makes it past the POST, the BIOS then locates a bootable partition and calls on the master boot record, which loads an operating system. [Figure 1-7](#) shows a BIOS chip on a motherboard. For more information on the system BIOS, refer to Book 2, [Chapter 4](#).





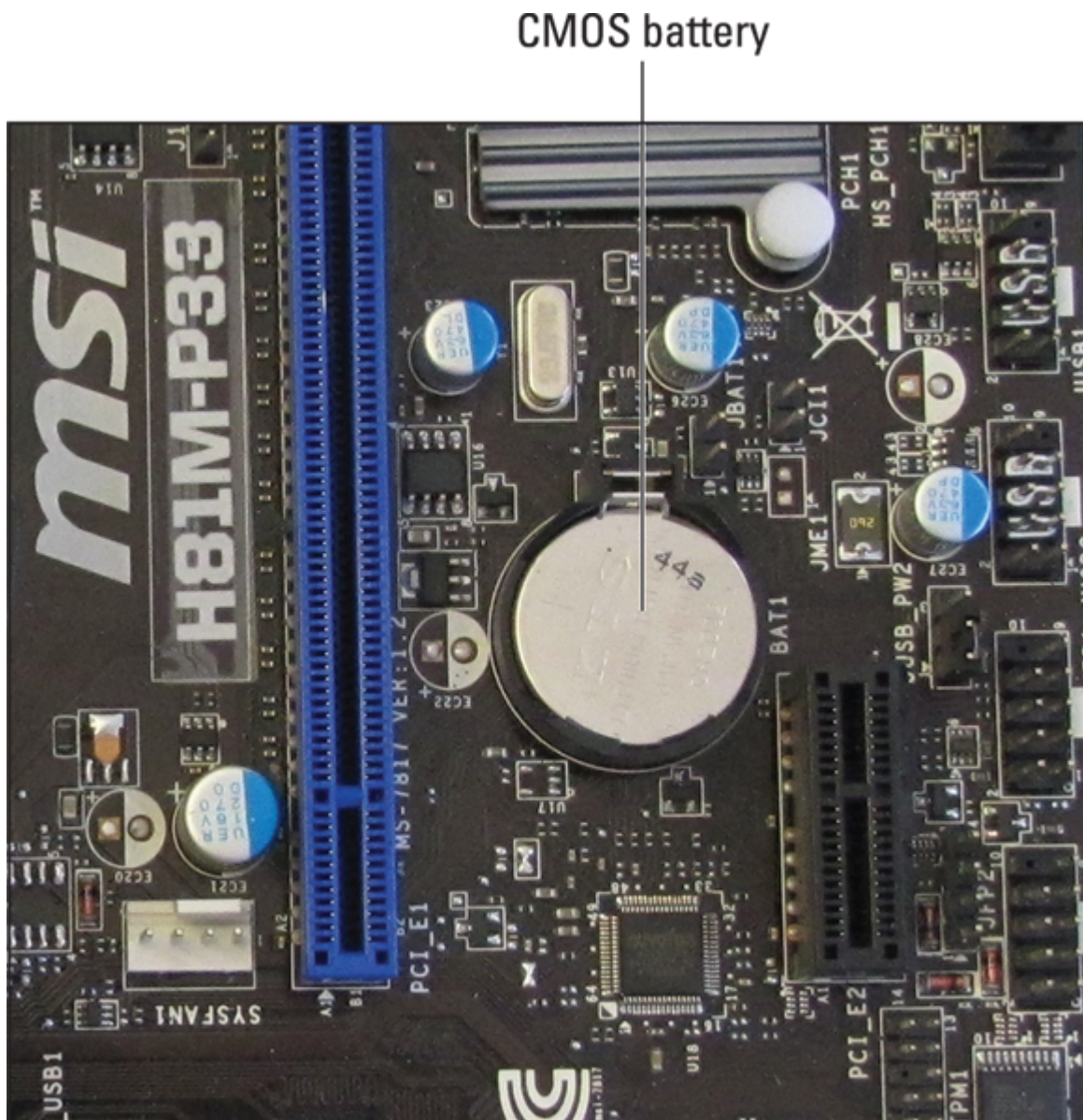
**FIGURE 1-7:** A BIOS chip located on the motherboard.

## *CMOS battery*

The computer keeps track of its inventory in what is known as the *complementary metal-oxide semiconductor (CMOS)*. CMOS holds a listing of system components, such as the size of the hard disk, the amount of RAM, and the resources (IRQs and I/O addresses) used by the serial and parallel ports.

This inventory list is stored in CMOS RAM, which is a bit of a problem because RAM loses its content when the power is shut off. You don't want the computer to forget that it has a hard disk or forget how much RAM it has installed. To prevent this sort of problem, a small watch battery on the motherboard maintains enough energy that CMOS RAM doesn't lose its charge. If CMOS RAM loses its charge, CMOS content is

lost. [Figure 1-8](#) identifies a CMOS battery on the motherboard. For more information on CMOS, check out Book 2, [Chapter 4](#).



**FIGURE 1-8:** The battery (on the motherboard) used to maintain a charge to CMOS RAM.

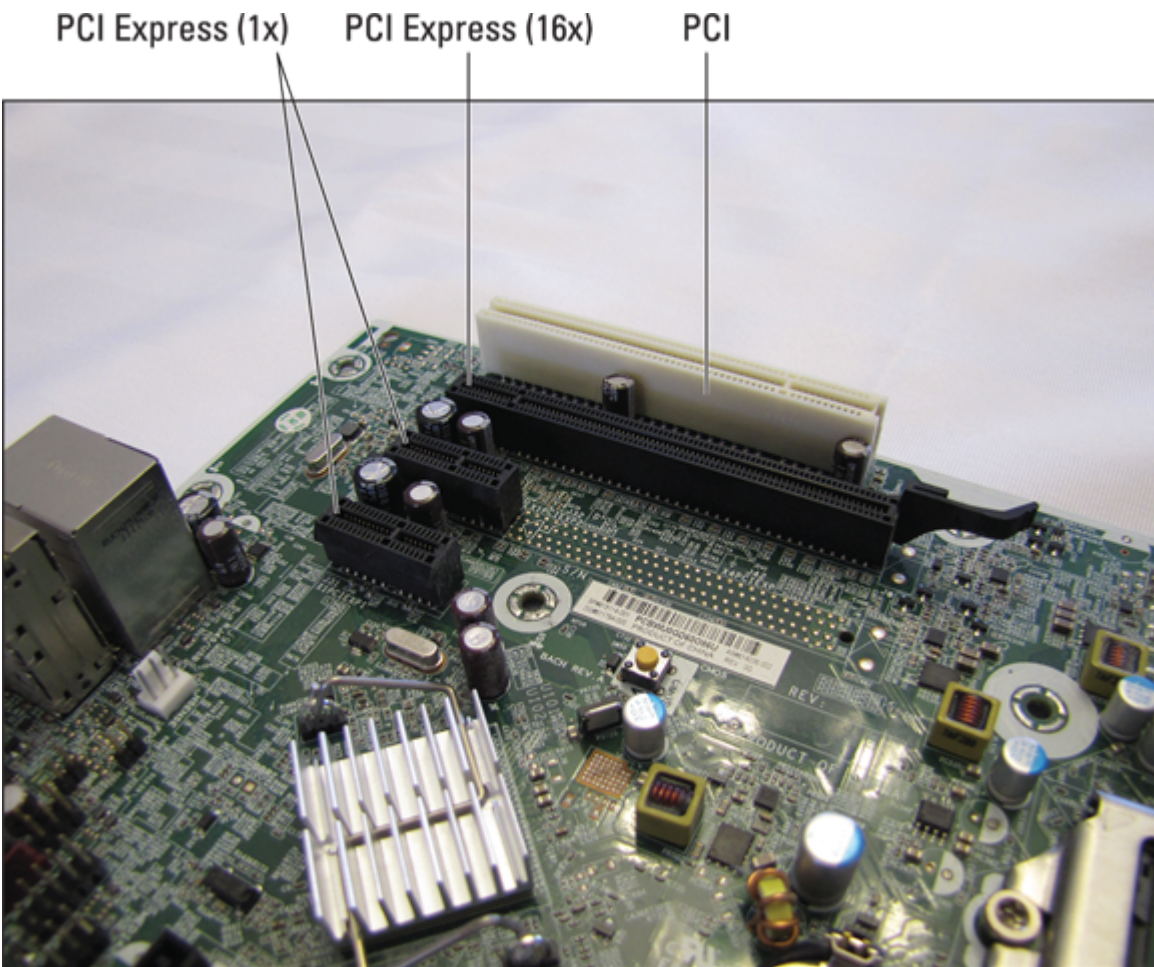
## *Expansion slots*

Most motherboards have one or more *expansion slots*, which add functionality to the computer. For example, assume that your computer doesn't have sound capability: You can install a sound card into the expansion slot to add that capability to your system.



Expansion slots come in different varieties, and it is extremely important to understand the benefits of each type. I discuss these issues later in the chapter, in the section titled “[Understanding Bus Architectures](#).” For now, I just want you to be able to identify the expansion slots on the motherboard.

If you look at the motherboard, you can see a number of expansion slots. There are probably some white, narrow PCI slots on the board, as well as black, narrow PCI Express slots (often used for video cards). You might also see some larger black PCI Express slots; these are better performing slots than the smaller PCI Express slots. [Figure 1-9](#) displays a PCI slot and two types of PCI Express slots: PCI Express 1x (smaller black slot), and PCI Express 16x (larger black slot). For more information on expansion slots, see “[Understanding Bus Architectures](#)” later in this chapter.

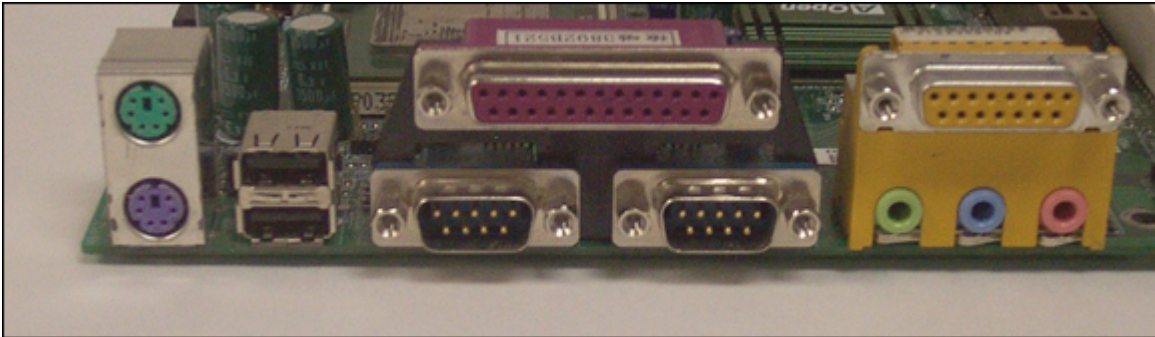




**FIGURE 1-9:** Expansion slots (PCI, PCIe 1x, and PCIe 16x) on a motherboard.

## *Ports and connectors*

A number of *ports* on the back of the motherboard connect the keyboard, mouse, printer, and other devices to the system. This section identifies those ports. [Figure 1-10](#) displays a number of built-in *input/output* (I/O) ports on the back of an ATX motherboard.



**FIGURE 1-10:** Built-in ports on the back of an ATX motherboard.

## *Serial ports*

Most motherboards have serial ports integrated directly into the board. The *serial ports* are also known as *communications (COM) ports*. They are called *serial ports* because they send data in a series — a single bit at a time. If eight bits of data are being delivered to a device connected to the COM ports, the system sends the eight bits of data, one bit at a time, in single file. Typically, there are two COM ports — COM1 and COM2 — on each system.

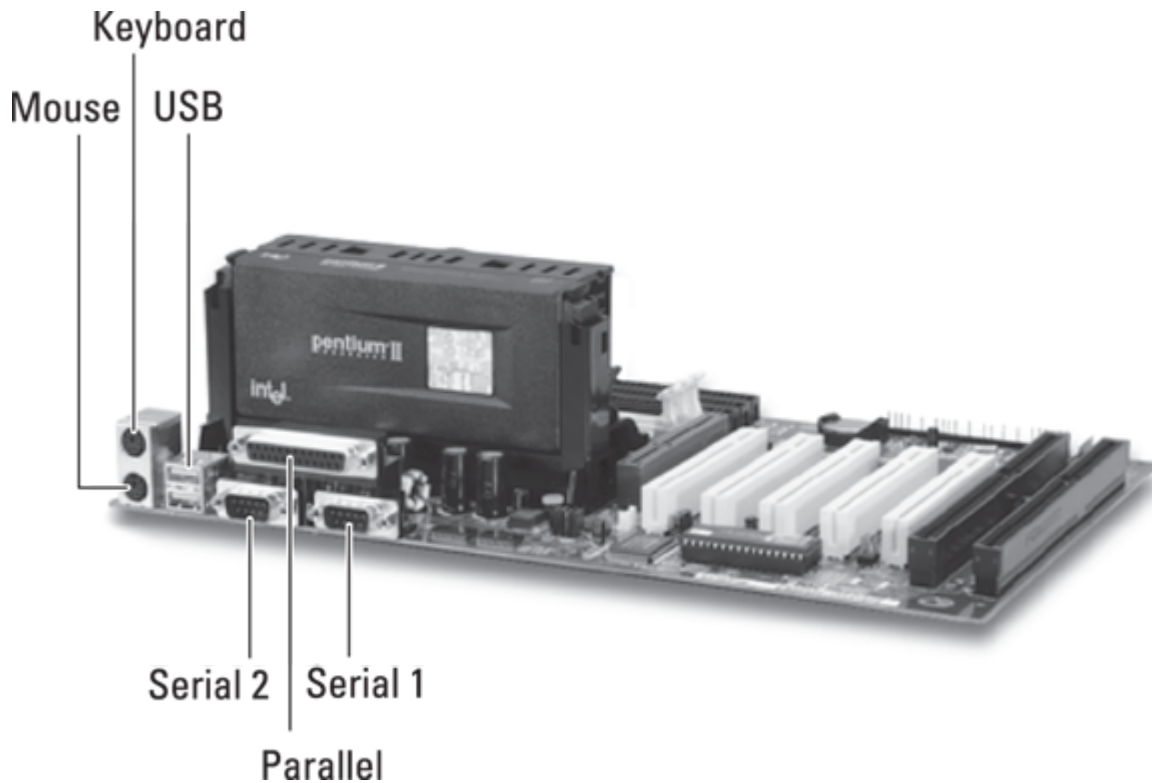


**FOR THE  
EXAM**

The official standard that governs serial communication is known as *RS-232*, and you might see serial ports referred to as *RS-232 ports*.

You usually connect an external modem or a serial mouse to a serial port. Each device is used for communication. For example, a modem allows your computer to talk to another computer across phone lines, and a serial

mouse allows you to communicate with the system. [Figure 1-11](#) shows two serial ports connected to a motherboard.



**FIGURE 1-11:** Integrated ports on the back of an ATX motherboard.

Serial ports on the back of the motherboard are one of two types:

- » **DB9-male:** A serial port with 9 pins
- » **DB25-male:** A serial port with 25 pins

### ***Parallel port***

Another type of connector on the back of a motherboard is the *parallel port*, also known as the *printer port*, or *LPT1*. The parallel port gets its name by being able to send information eight bits at a time. Whereas serial ports send only one bit at a time in single file, parallel ports can send eight bits in one operation — side by side, rather than single file. Refer to [Figure 1-11](#) to see a parallel port connected to a motherboard.

The parallel port, known as *DB25-female*, has 25 pin holes and is located on the back of the motherboard. Looking back at [Figure 1-11](#), you can see

the parallel port located above the two serial ports.



FOR THE  
EXAM

Do not confuse a serial port with a parallel port. A serial port is a *male* port (the port has a number of pins in it), whereas a parallel port is a *female* port (contains pin holes).

You connect the parallel port to a printer by using a parallel cable with a different type of connector at each end. On one end of the cable is a DB25 connector that attaches to the parallel port on the back of the computer. The other end of the cable (the end that connects to the printer) has a 36-pin Centronics connector.

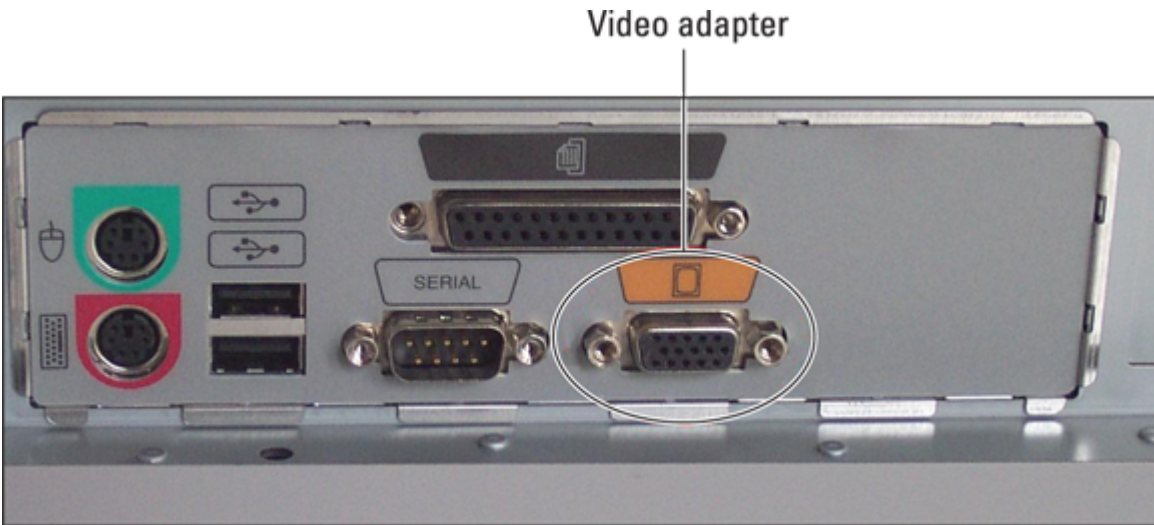


FOR THE  
EXAM

A standard printer cable has a different type of connector on each end. One end has a DB25-male connector with 25 pins, and the other end has a 36-pin Centronics connector.

### ***Video adapter***

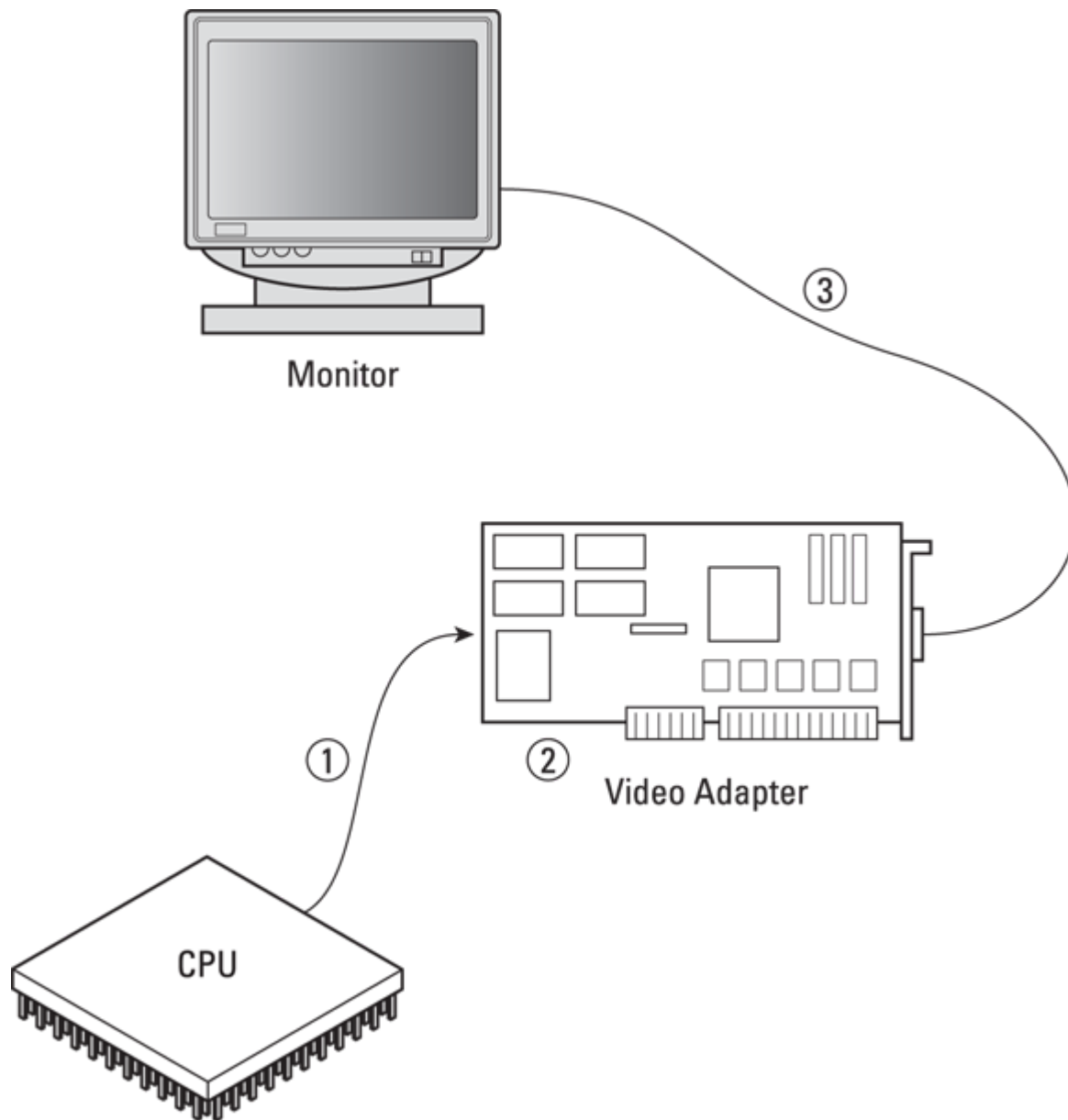
In the past, a motherboard came with a built-in *video adapter*, sometimes called a *video card* or *video controller*. The video adapter converts digital data from the processor and prepares the information to be displayed onscreen. [Figure 1-12](#) displays a video adapter port, which you can identify by the three rows of five pins. The VGA video port is a 15-pin female port.



**FIGURE 1-12:** A video adapter port.

Because many systems today use the ATX motherboard form factor, they have an AGP or PCIe slot to hold the video adapter. [Figure 1-13](#) shows how information flows from the computer system to the monitor. The following steps mirror the numbers in [Figure 1-13](#).

1. The video adapter is responsible for receiving digital data from the processor, which instructs the video adapter on how the images are to be drawn on the screen.
2. The video adapter stores the information about drawing the images in its memory and starts converting the information into analog data that the monitor can understand.
3. The data is sent in analog format from the video adapter to the monitor.



**FIGURE 1-13:** How information flows from the processor to the display.

### ***Keyboard/mouse connectors***

The mouse and keyboard connectors on motherboards today are most likely PS/2 style connectors or USB connectors. Focus on PS/2 connectors for now. A *PS/2* connector is a small, circular six-pin connector. In [Figure 1-14](#), you can see the keyboard and mouse connectors on the left side of the diagram.



Keyboard connector

Mouse connector

**FIGURE 1-14:** PS/2 connections for a keyboard and a mouse.

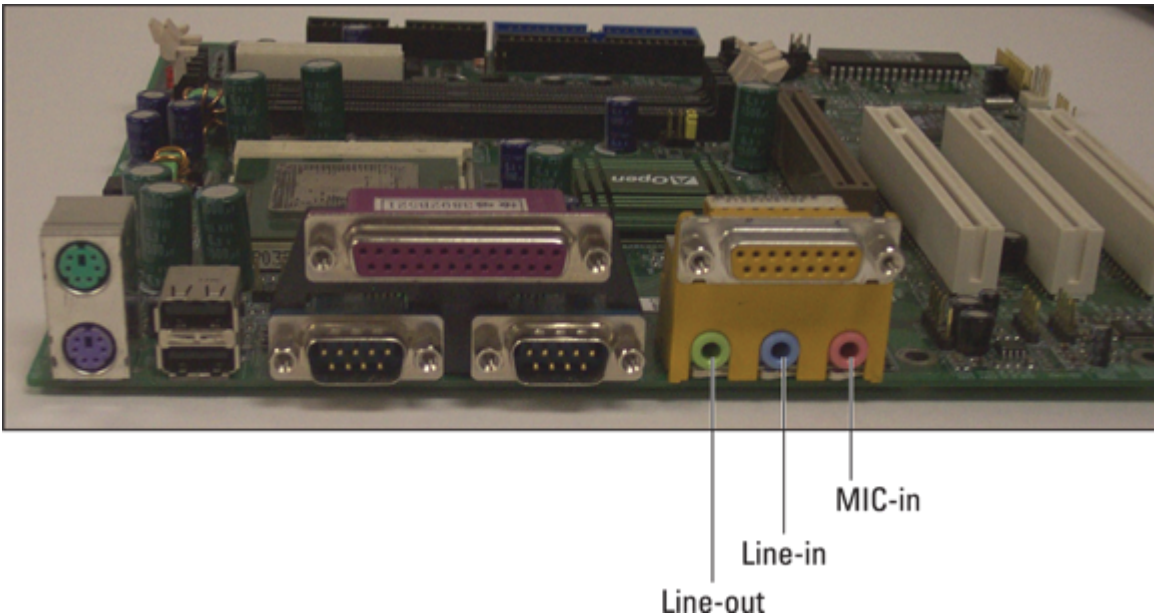
Most systems today use USB ports to connect the keyboard and mouse to the computer. You are not likely to see a PS/2 style connector on a new computer for the keyboard or mouse.

### ***Sound and front panel connector***

Most motherboards today have built-in sound capabilities, allowing you to connect speakers and a microphone to the computer. [Figure 1-15](#) shows the integrated sound ports on a motherboard. The three different ports on the integrated sound card are

- » **Line-in:** The line-in port (typically blue) allows you to connect many audio sources to the system.
- » **Line-out:** The speaker port (typically green) allows you to connect speakers to the computer.
- » **Microphone:** The MIC-in port (red) allows you to connect a microphone to the system for recording.



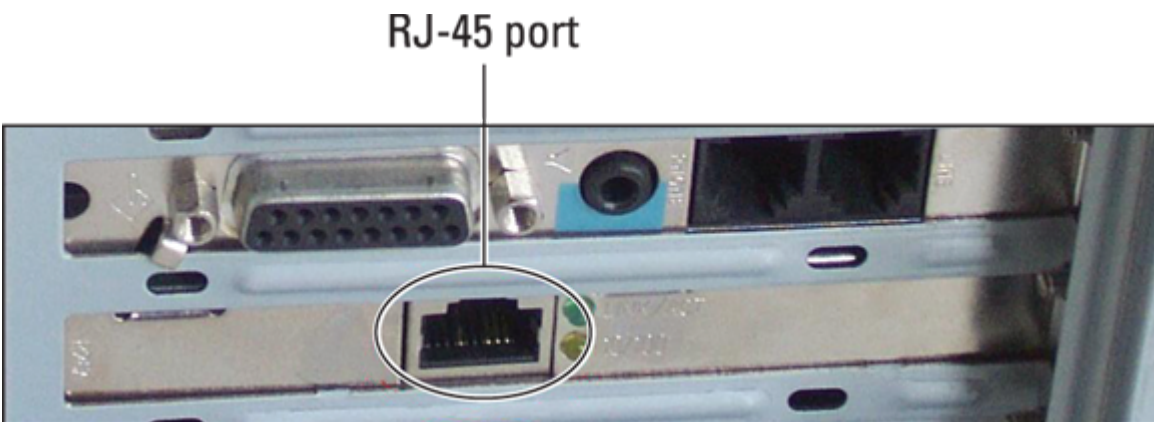


**FIGURE 1-15:** Sound ports on a system.

Note that the audio jacks on the front panel of the computer are functional only because they connect to the front panel connector port on the motherboard to provide communication to the audio ports.

### ***Network interface card and modem***

A number of systems today have built-in network support via an integrated *network interface card* (NIC), or network card for short. These systems might have a built-in modem as well. The built-in network card has an RJ-45 port on the back of the system that looks like an oversized telephone jack, as shown in [Figure 1-16](#).



**FIGURE 1-16:** An RJ-45 port.

The RJ-45 port on the back of the system board is used to connect to the network at speeds of 10 Mbps, 100 Mbps, or 1000 Mbps, which is why this is known as a 10/100/1000 port. It is possible to have a network port that offers a different speed, but those are the three common compatible speeds found in today's systems.

### ***USB ports and the Internal USB connectors***

*Universal Serial Bus (USB)* is a high-speed serial technology that transfers data at 12 Mbps (USB 1.0), 480 Mbps (USB 2.0), and up to 5 Gbps for USB 3.0. The newest USB standard known as USB 3.1 has a transfer rate of up to 10 Gbps! One of the major benefits of USB is the fact that all USB devices use the same type of connector, so you won't have to guess which ports to connect the mouse, keyboard, or scanner to. If they are all USB devices, they connect to the same type of port on the computer! Another huge benefit of USB is that the device receives power via the USB connection. This has the benefit of when connecting a device to the computer by the USB ports, you typically will not have a power cord for that device. Keep in mind that some devices are large enough that they still may require their own power source, such as a USB printer.

It should be noted that the USB ports on the front panel of your PC are connected to the motherboard by the 9-pin (for USB 1 or USB 2) internal USB connector found on the motherboard. USB 3.0 uses a 20-pin connector.



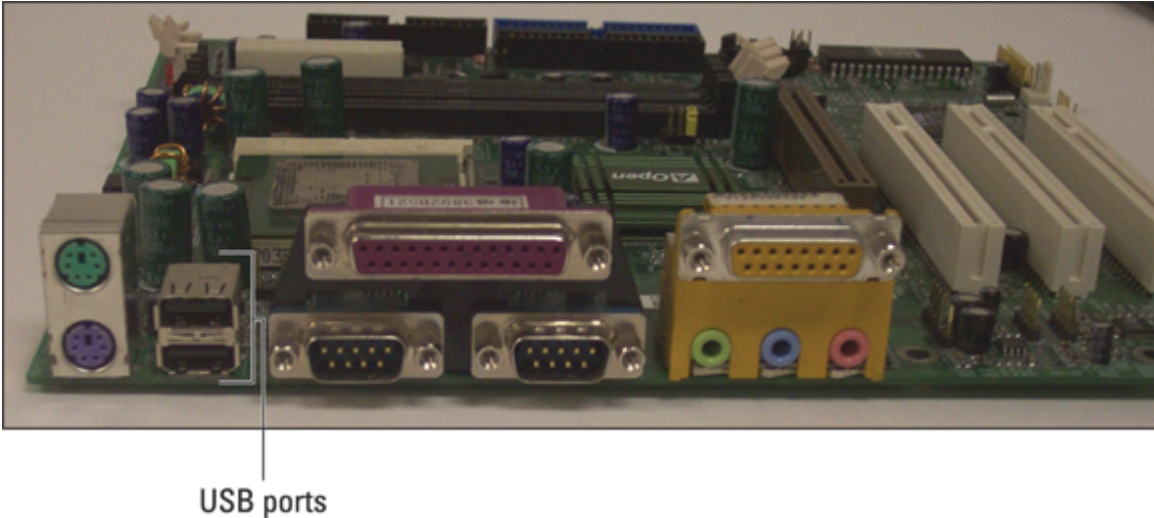
**FOR THE  
EXAM**

Be sure to know the USB standards for the A+ certification exams and know their transfer rates! Remember the following for the A+ exams:

- » **USB 1.0:** Transfers data at 12 Mbps.
- » **USB 2.0:** Transfers data at 480 Mbps.
- » **USB 3.0:** Transfers data at 5 Gbps.
- » **USB 3.1:** Transfers data at 10 Gbps.



USB devices also support *daisy-chaining*. For example, you can connect Device A to the back of the computer and then connect Device B to Device A, and so on. You can connect as many as 127 devices to a system using USB. [Figure 1-17](#) identifies the USB ports on the back of an ATX motherboard.



**FIGURE 1-17:** USB ports on the back of a motherboard.

A USB device that connects to the computer and then has other devices connected to it is considered a *hub device*. If you do not have a USB device that can act as a hub device, you can purchase a specific USB hub that allows you to chain four or more other devices off it. With a USB hub, you can easily increase the number of USB ports your system has by connecting USB devices to the hub and then connecting the hub to the back of the computer. [Figure 1-18](#) shows a USB hub.



**FIGURE 1-18:** A USB hub with four ports.

It should be noted that you can connect newer USB devices into older USB ports, but the downfall is you will only get the transfer rate of the oldest version. For example, if you connected a USB 3.0 device to a USB 2.0 port then you would only get the 480 Mbps.

### ***FireWire (IEEE 1394)***

When USB 1.0 was introduced, it ran at 12 Mbps. This was a fairly good speed for most types of devices but was a little too slow when it came to multimedia devices, such as digital video cameras. Typically, these types of devices use a *FireWire* serial connection, which has a transfer rate of up to 400 Mbps and supports 63 devices in a chain. This initial version of FireWire is IEEE 1394a, which is also known as FireWire 400.



**FOR THE  
EXAM**

The official standard that defines FireWire is known as the IEEE 1394. Like USB, it has been improved over time and has different versions. Be sure to know the different FireWire standards for the A+ exams.

Just like USB has different versions with faster transfer rates, so does FireWire. The second version of FireWire is defined as the IEEE 1394b

standard and transfers data at 800 Mbps! This second version of FireWire is also known as FireWire 800.

The next step in the FireWire standard was to jump to S1600, which ran at 1.57 Gbps. Then next standard, S3200, had a transfer rate of 3.14 Gbps. You may be wondering why the name begins with the letter *S*? Remember that FireWire is a serial technology, so *S* stands for *serial*.

[Figure 1-19](#) shows a digital video camera being plugged into a FireWire port.



**FIGURE 1-19:** A digital video camera being connected to a system by the FireWire port.



FOR THE  
EXAM

For the A+ exams, remember that the original version of FireWire runs at 400 Mbps and is known as IEEE 1394. The second version of FireWire, FireWire 800, is also known as IEEE 1394b but runs at 800 Mbps. After those versions you have the S1600, which runs at 1.57 Gbps, and the S3200, which runs at 3.14 Gbps. Also, remember that FireWire supports 63 devices in a daisy chain.

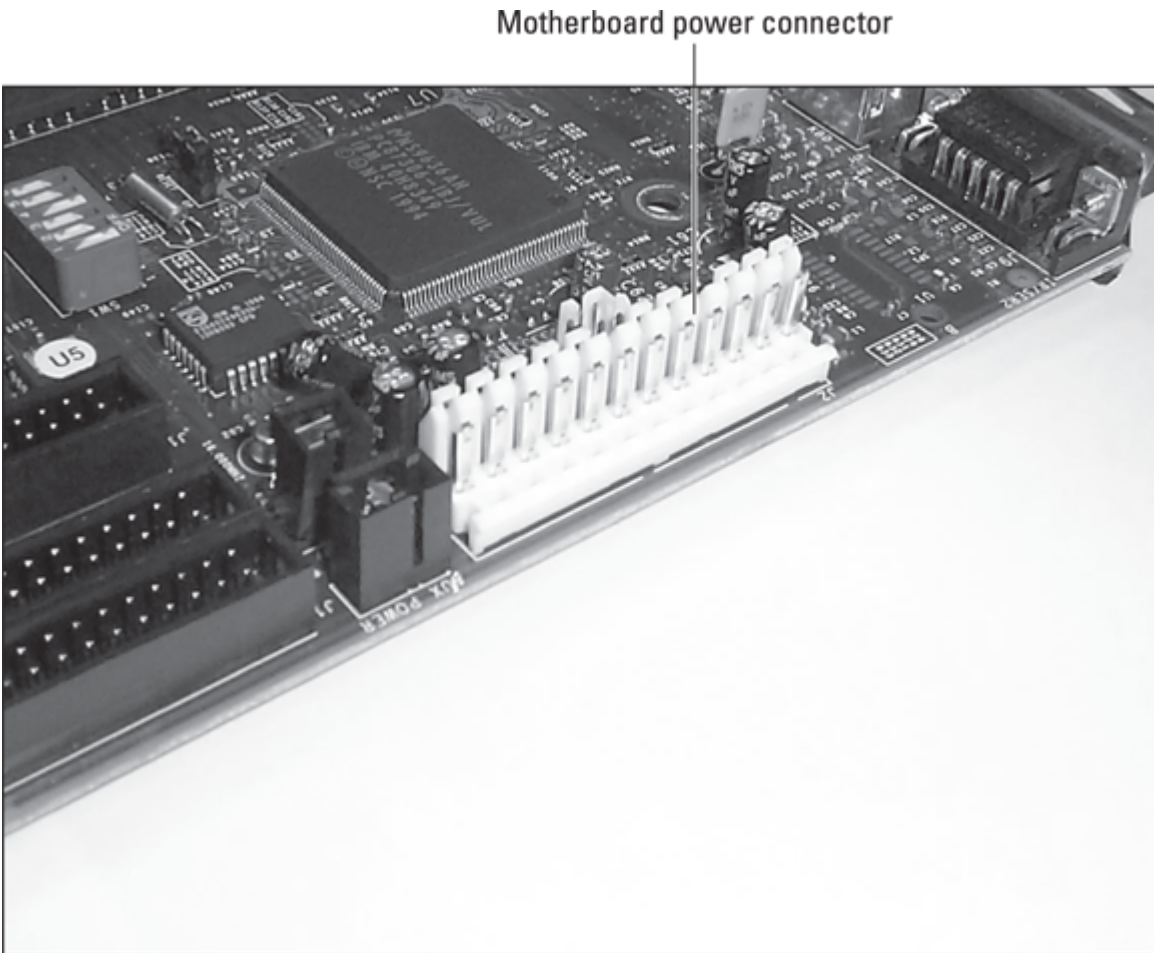
For more information on common ports and connectors — such as keyboard, mouse, serial, parallel, USB, and FireWire — read Book 3, [Chapter 1](#).

## *Power connections and types*

All the devices connected to the motherboard need to get power from somewhere, so the power supply is connected to the motherboard, which supplies power to the board and its components. The following sections discuss power connectors on older and newer motherboards.

### *Older motherboard power connectors*

[Figure 1-20](#) shows power connectors on an older motherboard. There are power cables coming from the power supply to connect to the motherboard with very unique connectors on the end. These power connectors coming from the power supply that connect to the motherboard may be labeled as P1 and P2, or on some systems, P8 and P9.



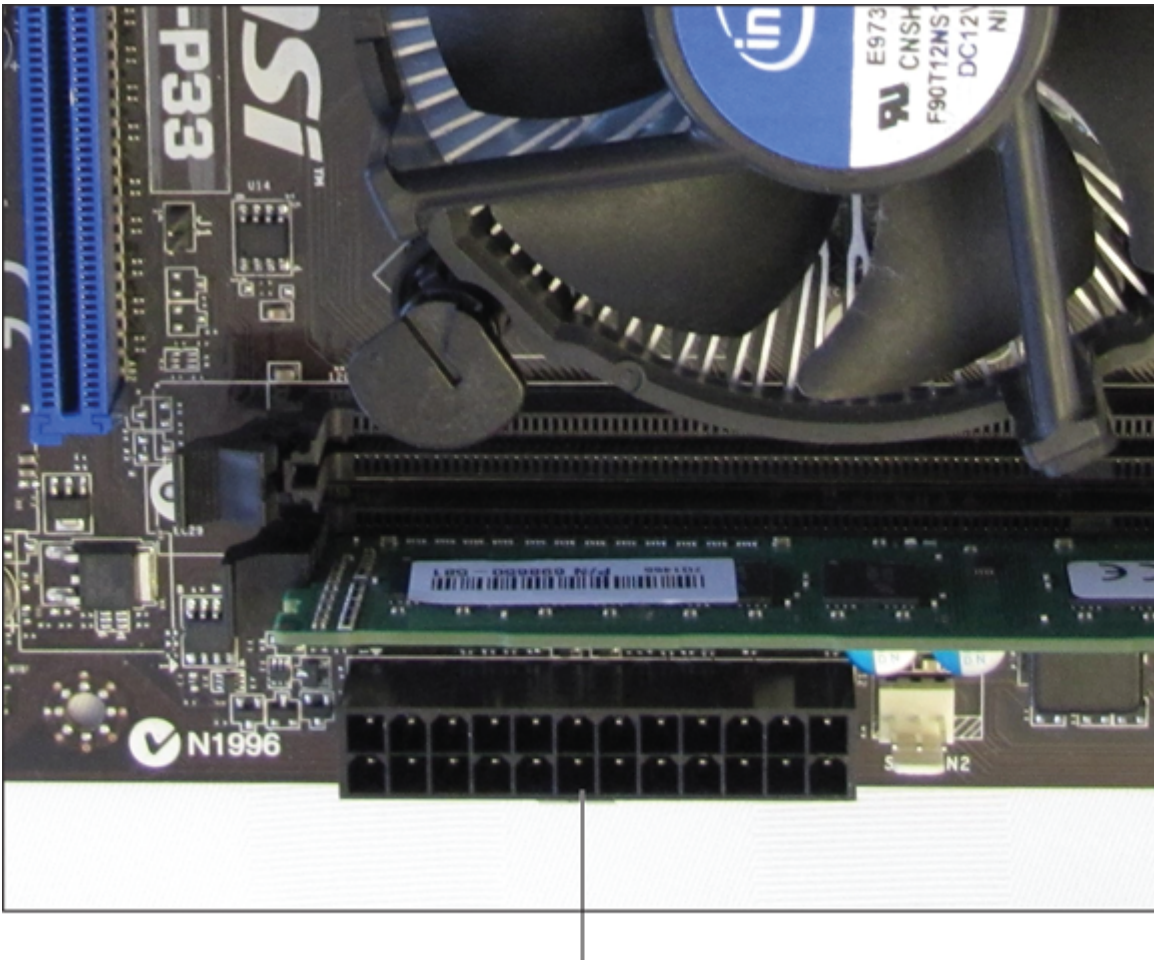
**FIGURE 1-20:** Power connectors on an older motherboard.

You have to be extremely careful to make sure that the connectors on the cable coming from the power supply to the motherboard are inserted properly, or you could damage the motherboard. Often, these connectors are *keyed* (meaning that they can go in only one way) so that you cannot put both of the connectors in the wrong way. These older power connectors supplied power in 5 volts (V) and 12V.

### ***ATX power connectors***

Newer ATX motherboards use a different power connector than the one shown in the preceding section. The ATX power connector supplies 3.3V, 5V, and 12V. The ATX power connector, shown in [Figure 1-21](#), is typically labeled as P1 and is a 24-pin connector.





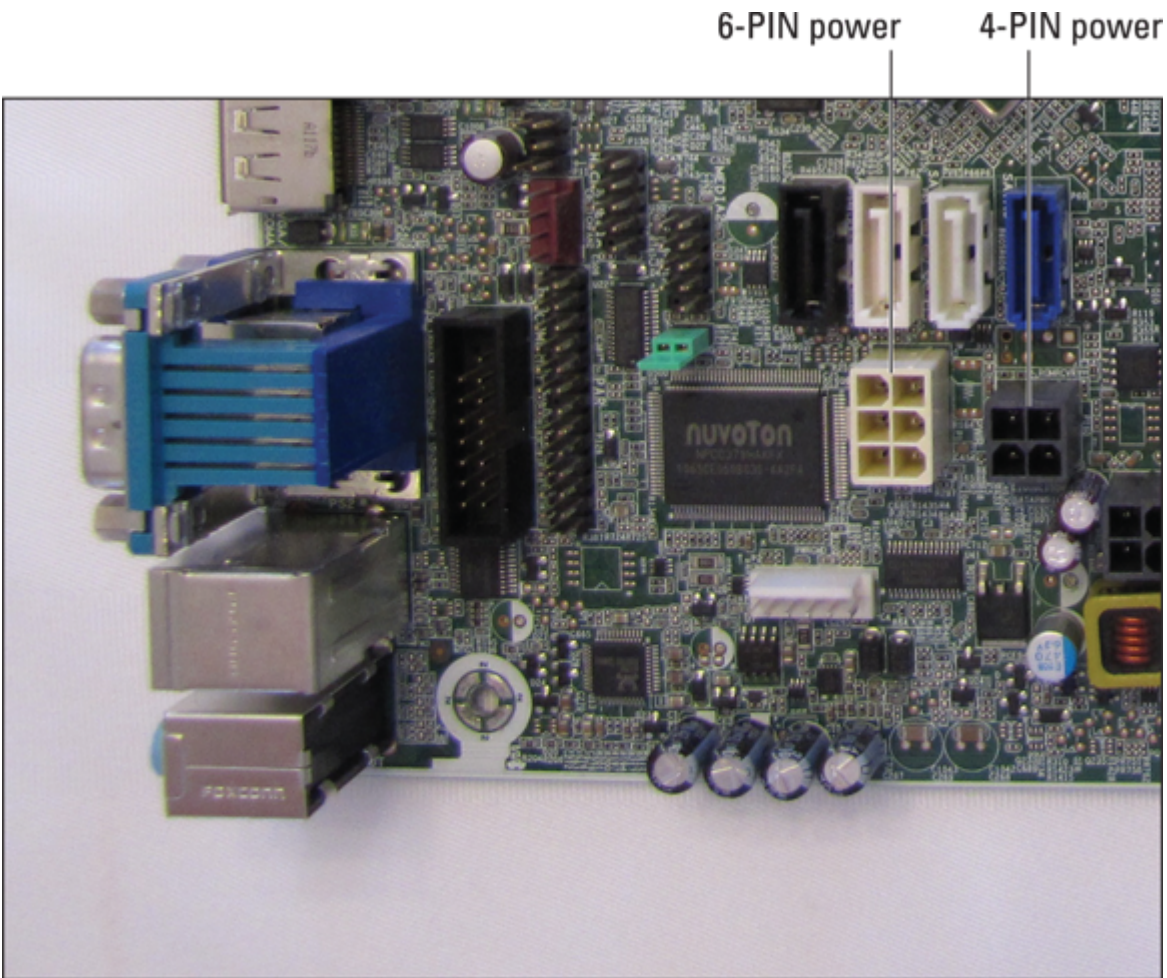
ATX 24-PIN power connector

**FIGURE 1-21:** The ATX power connector on an ATX motherboard.

Most motherboards today use an extra power connector to supply power to additional components connected to the motherboard. A common connector is known as the P4 power connector, which supplies an additional 12V to the CPU. The P4 connector gets its name from having 4 pins.

### ***PCIe 6-PIN power connector***

Another power connector you may find on your motherboard or graphics card is the 6-PIN power connector, which is used to supply additional power to your graphics card or GPU. The graphics cards today are typically PCIe cards inserted into the PCIe 16x slot on the motherboard. The 4-PIN and 6-PIN power connectors are shown in [Figure 1-22](#).



**FIGURE 1-22:** 4-PIN and 6-PIN power connectors on an ATX motherboard.



**TIP** If you need a 4-PIN or 6-PIN connector on your power supply, but one does not exist, you can purchase adapters to convert the Berg connector on the power supply to a 4-PIN or 6-PIN connector.

### *Fan power connectors*

Located on the motherboard you should also see a place to connect the fans to the motherboard so that the fans can receive power from the motherboard to run. These power connectors are usually small connectors located around the edge of the motherboard.



**TIP**

For more information on power supplies and their connectors, check out Book 2, [Chapter 6](#).

## ***Drive connectors***

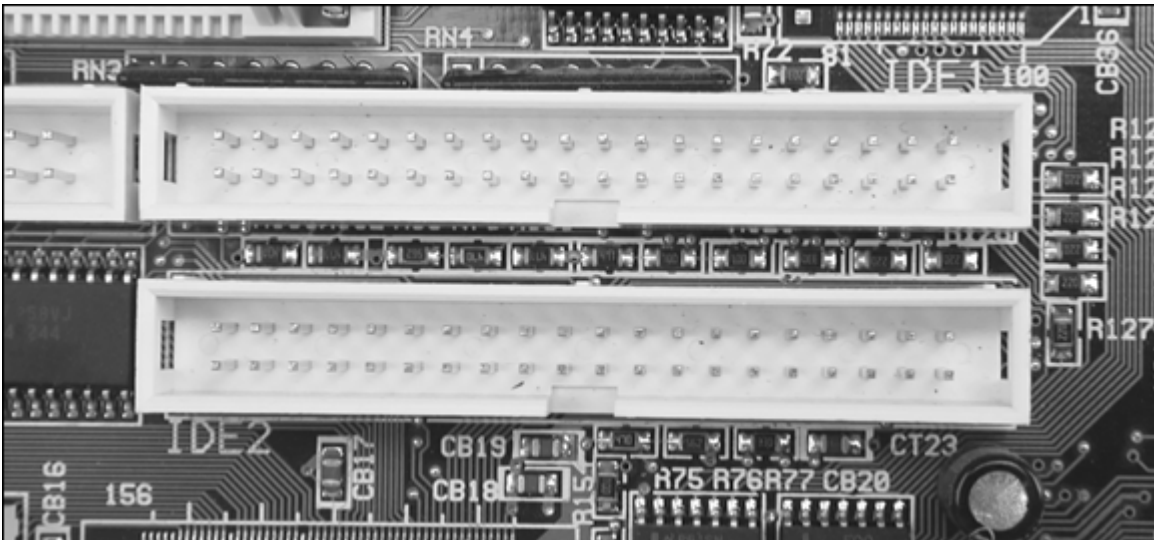
You need to be able to identify the different types of connectors that link hard drives to your system. As you might already be aware, the hard drives are used to store information permanently on the computer, but to access that information the drives have a physical connection to the system via the motherboard.

The four major types of drives in systems today are EIDE (Enhanced Integrated Drive Electronics), SATA (Serial Advanced Technology Attachment), SCSI, and floppy drives. Each type of drive has its own type of connection on the motherboard. Before you purchase a hard disk to add to the system, you need to be aware of what types of drives your motherboard supports.

### ***IDE/EIDE connections***

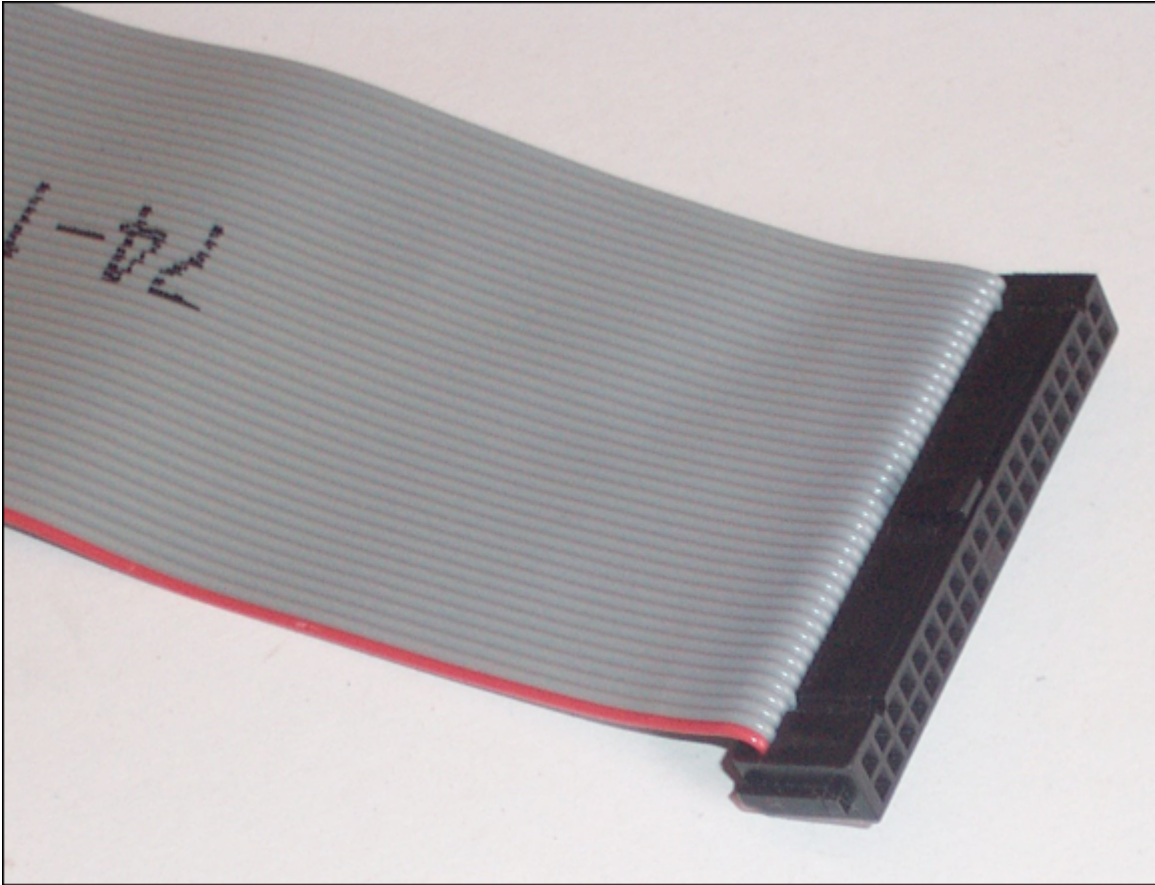
IDE drives have been around since the 1980s, and although the technology has improved from a performance perspective, IDE drives connect to the system the same way they always have. IDE was improved to become EIDE but essentially the underlining technology is the same with a few improvements, such as IDE supported two devices in a chain while EIDE supported four devices in a chain. If your motherboard supports EIDE, you will have two EIDE connectors that are made up of 40 pins each, as shown in [Figure 1-23](#).





**FIGURE 1-23:** EIDE connectors on the motherboard.

You connect the drive to the connector on the motherboard by using a 40-wire or 80-wire EIDE ribbon cable. This ribbon cable typically has two connectors on it — one end connects to the drive and the other end connects to the motherboard. You can also find EIDE ribbon cables with three connectors that allow you to connect two drives to each EIDE connector on the motherboard. This means that you can have up to four EIDE devices on a system. [Figure 1-24](#) shows an EIDE ribbon cable connector.



**FIGURE 1-24:** A 40-wire EIDE ribbon cable.

When connecting the EIDE ribbon cable to the drive and motherboard, the colored wire on the ribbon cable connects to pin 1 on the connector. This is the *pin-1 rule*. Pin 1 is normally labeled on the motherboard and drive. If it isn't labeled, see whether the manufacturer has labeled pin 40 — if so, pin 1 is at the other end!



TECHNICAL  
STUFF

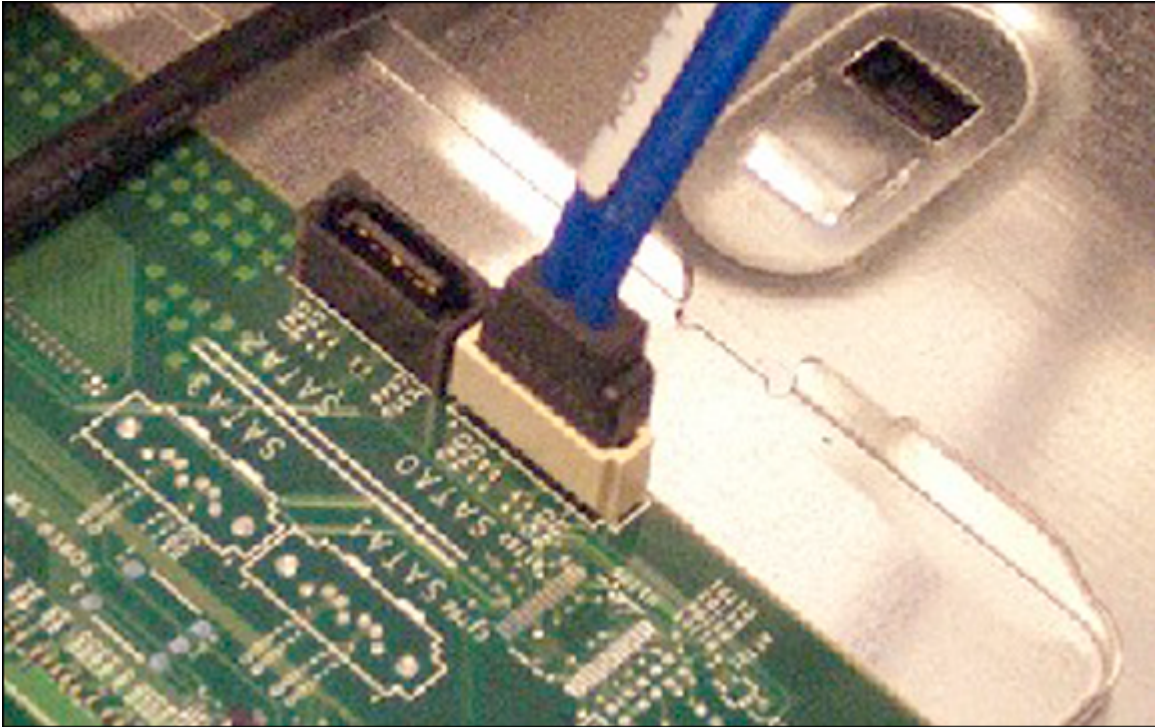
*EIDE controllers* is a popular term used in the computer industry for the EIDE connectors. Although in theory, these are not controllers, this term is used in the industry to describe the EIDE connections on the motherboard. The *actual* EIDE controller — the circuitry located on the circuit board on the drive itself — is responsible for controlling the flow of information to and from the drive.

## ***SATA connections***

Limitations of the EIDE architecture have kept its data transfer rate around 150 MBps. As drives become more powerful, a new standard was needed. The first new standard to replace EIDE — SATA — is the popular drive technology in desktop, laptops, and even some network servers. SATA has evolved over time and has some really good transfer rates:

- » **SATA 1.0:** Transfers data at 1.5 Gbps (150 MBps), which is the equivalent of high-end IDE technology
- » **SATA 2.0:** Transfers data at 3 Gbps (300 MBps)
- » **SATA 3.0:** Transfers data at 6 Gbps (600 MBps)
- » **SATA 3.2:** Transfers data at 16 Gbps (1969 MBps)

SATA uses its own unique four-wire cable to connect to the motherboard. [Figure 1-25](#) shows a SATA cable connected to the SATA connector on the motherboard. Notice that the cable is quite a bit thinner than the EIDE ribbon cable; this allows for better airflow in the system and improves overall temperature control of the computer.



**FIGURE 1-25:** A SATA cable connected to the motherboard.



**REMEMBER** Unlike EIDE drives, you cannot connect more than one SATA drive to a connector. For example, if your motherboard has two SATA connectors, you can connect only two SATA drives to the system unless you purchase a SATA card that has additional connectors.

SATA is a hot-swappable technology that allows you to remove and add drives while the system is still running. This adds huge benefits over EIDE solutions.

### ***eSATA connections***

eSATA (External SATA) allows for external drives to connect to a system via a SATA port instead of the typical USB or FireWire port. In the past, external drives were enclosures that held SATA drives, but the interface to connect the enclosure to the computer used USB or FireWire. This created overhead because the SATA interface is translated to USB or FireWire, which is slower than SATA. With eSATA connections on the

motherboard, you can connect to the external drive using eSATA to leverage SATA speeds with no translation drawbacks!

The eSATA device, which requires its own power source because it is an external device, can have an external SATA cable length of two meters. The eSATA cable is a special cable designed to help prevent electromagnetic interference (EMI). The eSATA cable has also been designed to handle more than 5,000 insertions and removals of the drive; the current internal SATA cable is suited for only 50 insertions and removals.



**TIP**

If your motherboard does not have an eSATA port, you can purchase an expansion card to add to the computer, providing the eSATA ports.

### ***SCSI controller***

Some high-end machines, particularly those designed for use as servers, might have a controller on the motherboard with 50 pins on it. This is the footprint of a *SCSI (Small Computer System Interface) controller*. Because SCSI devices outperform IDE devices, SCSI controllers are extremely popular for servers (which have greater hard disk access and storage needs than regular desktop computers). To connect a SCSI drive to the 50-pin SCSI connector on the system, you use a 50-wire ribbon cable.



**FOR THE  
EXAM**

EIDE uses a 40-pin connector that a 40/80-wire ribbon cable connects to, and an internal SCSI connector has 50 pins that connect to a 50-wire ribbon cable.

### ***SAS connectors***

Another type of hard drives that you may find in servers is *Serial Attached SCSI (SAS)*. SAS is a serial technology that supports transfer rates of up to 12 Gbps and uses a thinner cable type than SCSI. SAS

supports the installation of 128 devices in the bus as compared to SCSI, which supports 16 devices.



ON THE  
WEB

Lab 1-1 and Lab 1-2 will help you identify the major motherboard components on the motherboard. Lab 1-1 and Lab 1-2 can be found on the companion website at

[www.dummies.com/go/aplusaio](http://www.dummies.com/go/aplusaio).



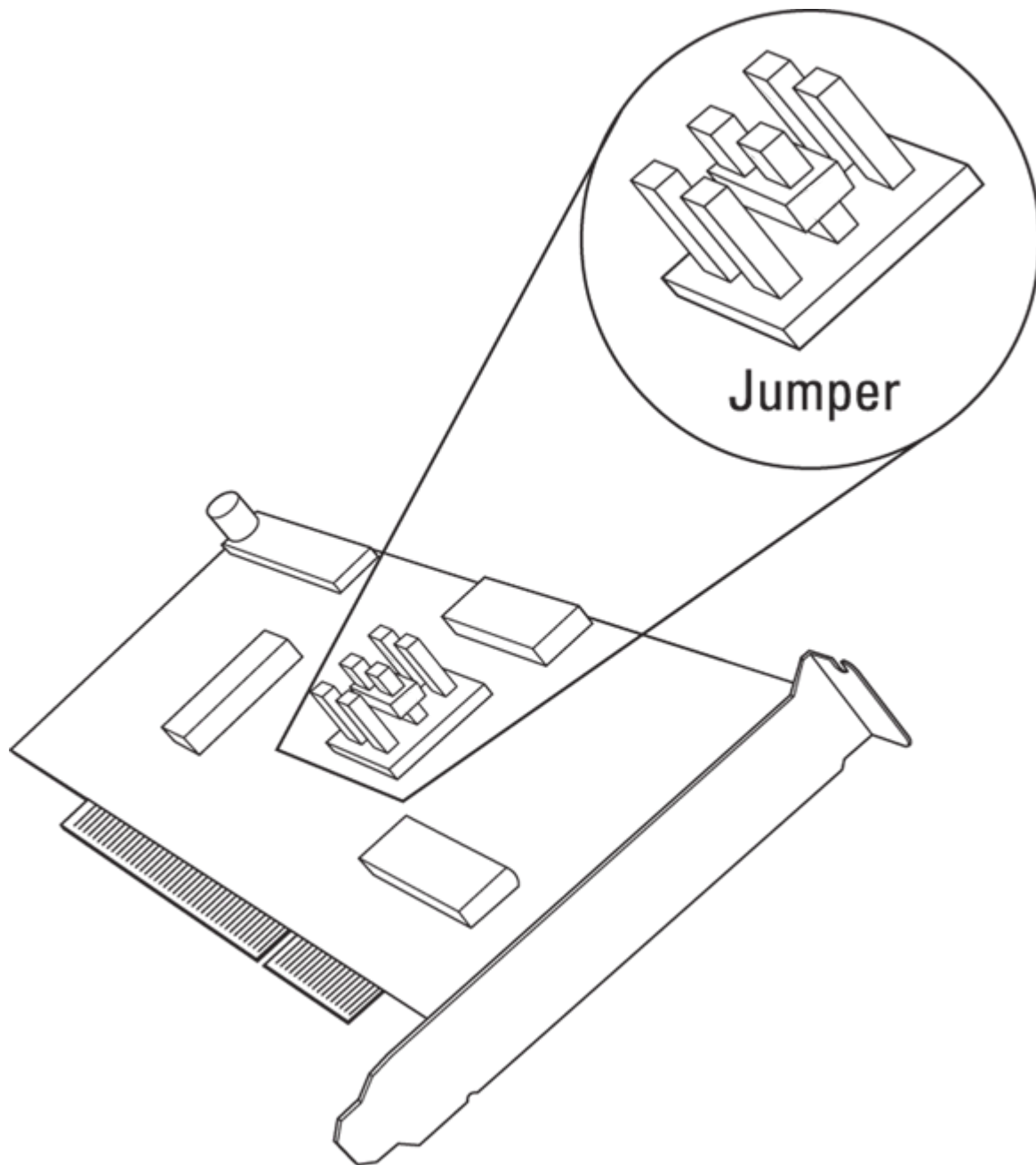
TIP

To find out more information about EIDE, SATA, and SCSI drives, check out Book 2, [Chapter 5](#).

## ***Jumpers and DIP switches***

A  *jumper* is a set of pins that have a plastic cap enclosed over them to create an electrical connection. The plastic cap contains a piece of metal that makes contact with the pins and creates the electrical circuit. The circuit that is created enables a feature on the motherboard. Most motherboards (and older expansion cards) use jumpers to implement different settings. [Figure 1-26](#) displays a jumper on an expansion card.





**FIGURE 1-26:** Identifying a jumper.

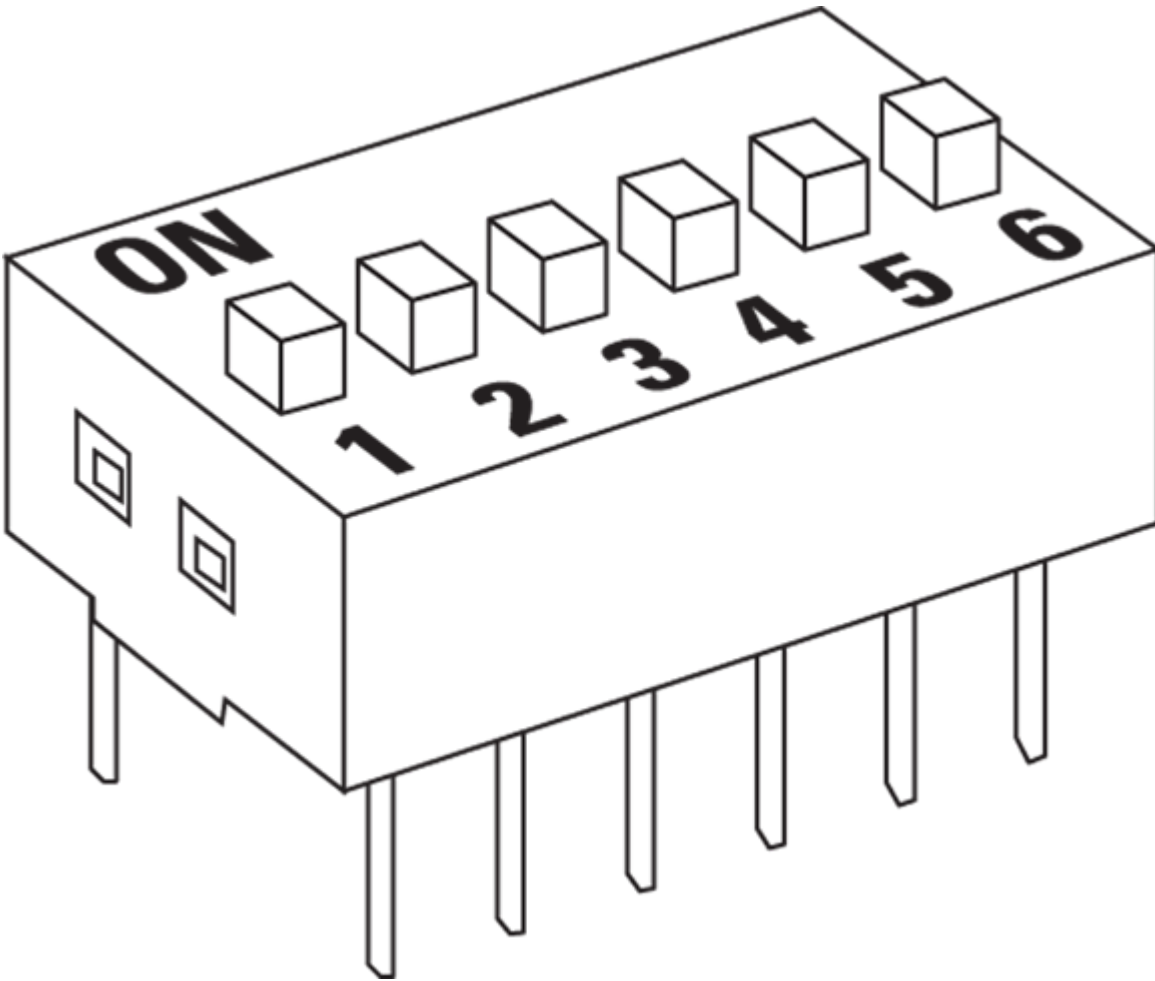
Notice in the figure that the jumper has three sets of pins that the cap may be placed over. The idea behind the three sets of pins is that each set of pins would enable a different setting. For example, looking at [Figure 1-26](#), the three different sets of pins might be used to assign three different interrupt requests (IRQs) to the card. You choose which IRQ is assigned

to the card by setting the jumper over a set of pins. Keep in mind that you no longer assign IRQs with jumpers; that was something done years ago.

Today, you find jumpers on motherboards, hard drives, DVD-ROM drives, and DVD drives. Many different features can be enabled or disabled on a motherboard by using jumpers. For example, there usually is a jumper on the motherboard used to clear the CMOS password of a system, to change the voltage supplied to the processor socket, or to change the speed of the motherboard. To know what jumper to set, check the documentation for the motherboard.

Another popular component of a motherboard or expansion cards in the past that was used to enable or disable different features is the dual inline package (DIP) switch. A *DIP switch* (as shown in [Figure 1-27](#)) is a set of switches that can be turned on or turned off to enable functionality on the board. To know what to set for on/off combinations, consult the documentation for the board.





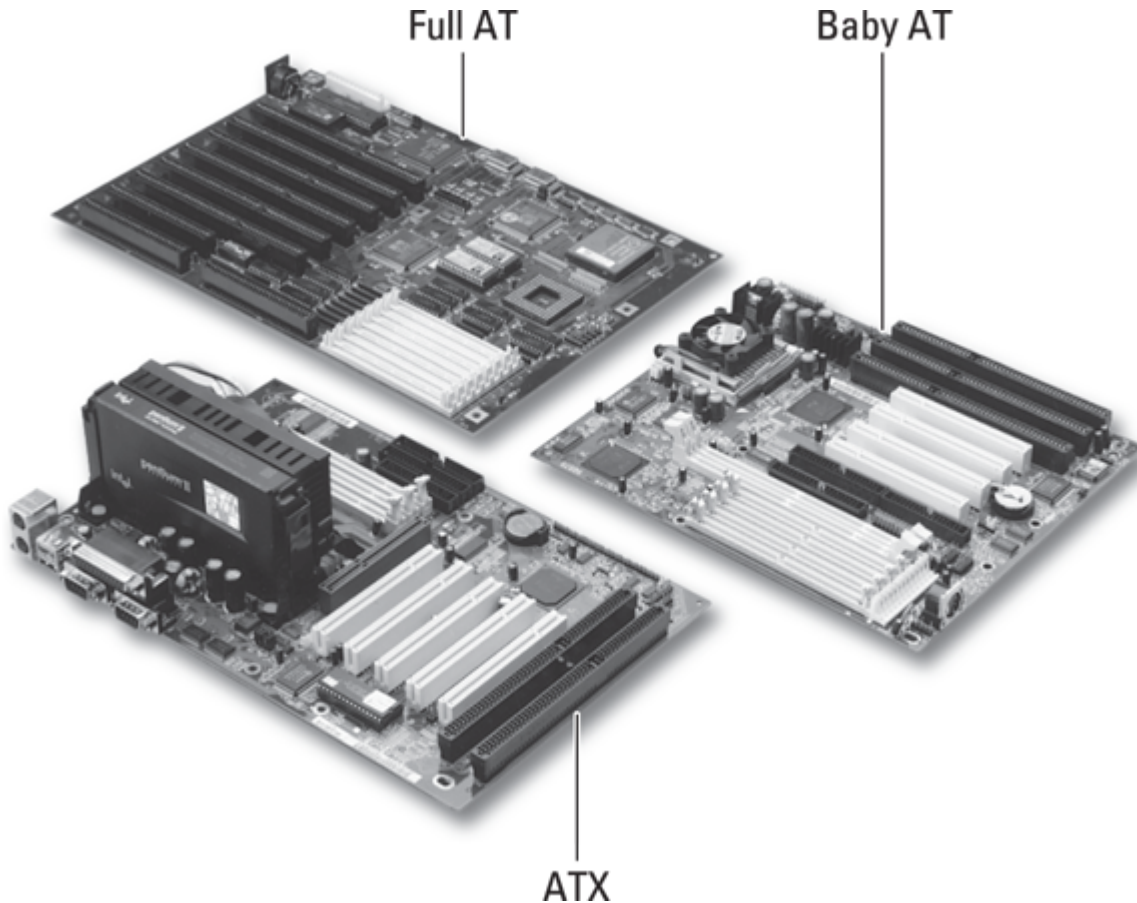
**FIGURE 1-27:** A DIP switch.

## *Identifying the Types of Motherboards*

Now that you understand some of the major components of the motherboard (system board), it is important to mention the different motherboard form factors. A *motherboard form factor* just describes the dimensions of the motherboard and the layout of the motherboard components.

You need to understand the different motherboard form factors because you can't just take *any* motherboard and place it in a computer case. For example, you must put an ATX motherboard in an ATX case, and put an

LPX motherboard in an LPX case. [Figure 1-28](#) shows some older motherboards to give you an idea of size and shape differences between different motherboards.



**FIGURE 1-28:** Looking at different motherboard form factors.

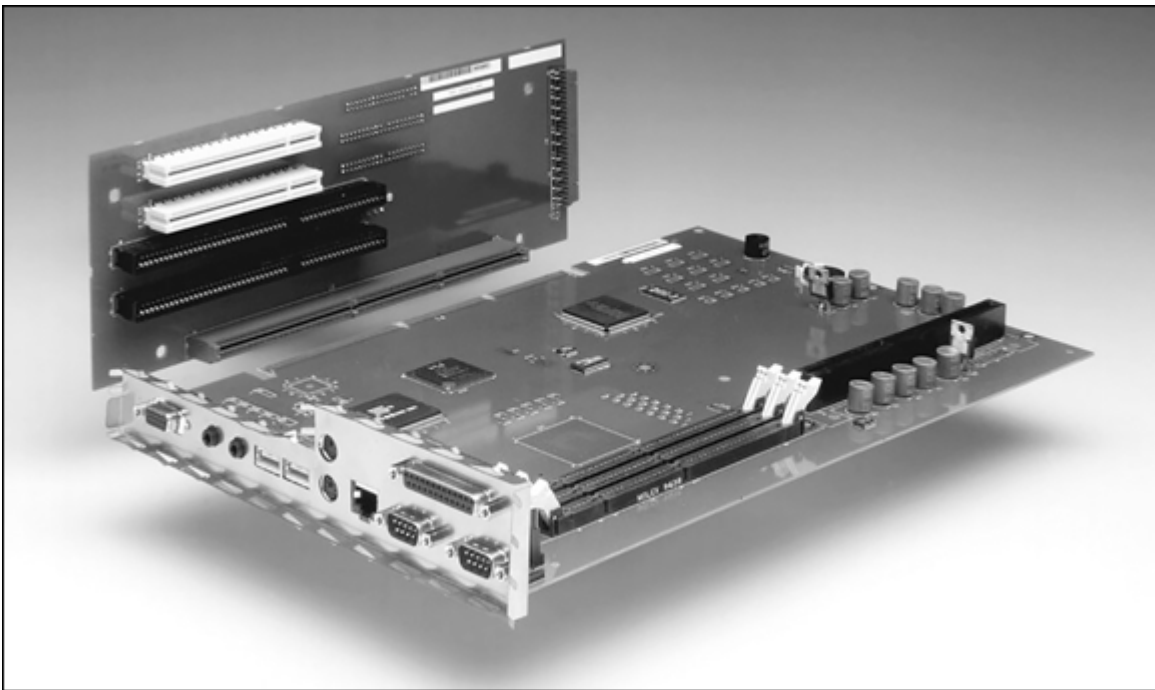
## ***LPX/NLX***

In an effort to allow computers to take up much less space, a slimline desktop system was designed with a smaller motherboard. After the era of older motherboards such as the Baby AT came the LPX (low profile extended), which was then replaced by NLX (new low profile extended) motherboard. Both motherboard types served the same purpose — to create low-profile computers.

The NLX motherboard is identifiable by the I/O ports along the back of the motherboard. This motherboard is unlike the full and Baby AT because they incorporated only the keyboard connector. Comparatively,

the NLX provides a keyboard and mouse connector, serial and parallel ports, and a video connector.

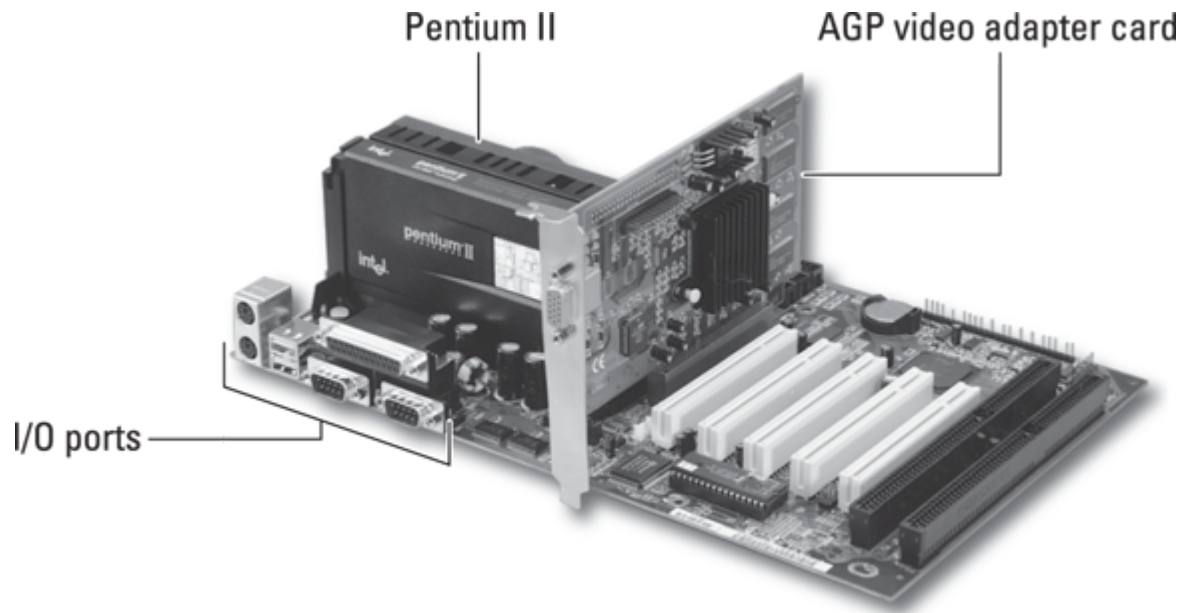
The NLX form factor — 9 x 13.6 inches — uses a riser card to house the bus architectures. The riser card typically connects to the side of the motherboard and is then secured along the side of the case. [Figure 1-29](#) shows an NLX motherboard with a riser card. (I cover bus architectures in the section, “[Understanding Bus Architectures](#),” later in this chapter.)



**FIGURE 1-29:** An NLX form factor motherboard.

## *ATX*

In 1995, Intel wanted a motherboard that would support the Pentium II processor and the new AGP slot, so the ATX form factor was built (shown in [Figure 1-30](#)). The ATX board — 7.5 x 12 inches — has most of the I/O ports integrated directly into the board, including USB ports.



**FIGURE 1-30:** The position of the I/O ports on an ATX motherboard.

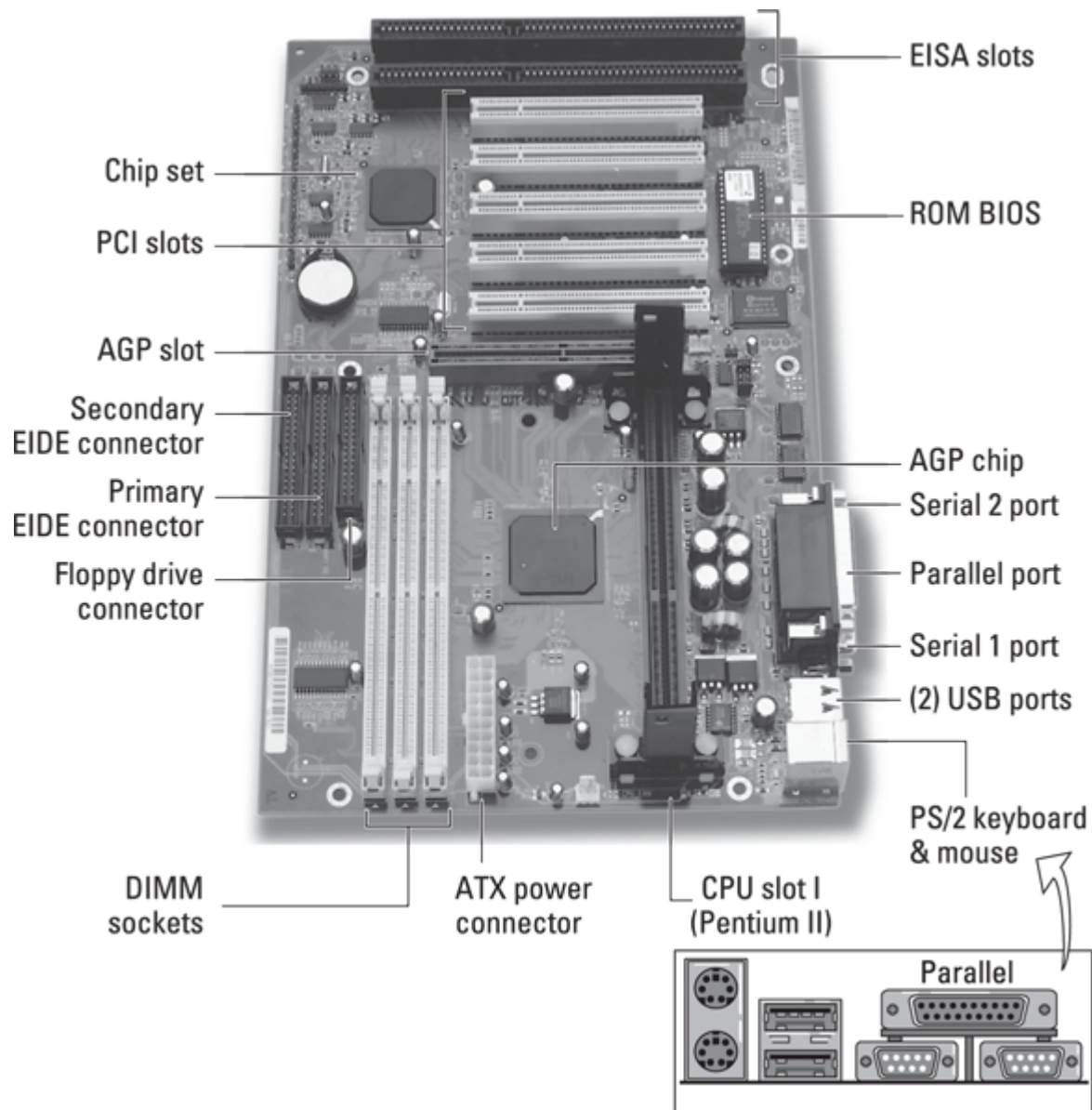


**FOR THE  
EXAM**

The ATX motherboard incorporates the I/O ports and includes an AGP slot for high-performance video cards. [Figure 1-30](#) displays the ports on the back of the ATX motherboard. Note how they are clustered in the left corner of the board and do not spread across the length of the board like they do with the NLX form factor.

The ATX board introduced a 100 MHz system bus and has been increased to speeds of 533 MHz and higher. The ATX motherboard originally had one AGP slot for the video card, which means that the built-in I/O ports on the back of the board do not have a built-in video card like the NLX. The ATX board also has *soft power support*, which allows software developers to create software that controls the startup and shutdown of the system.

The ATX form factor rotated the Baby AT components by 90 degrees so that any cards inserted into the bus architectures would not cover the processor and prevent proper cooling. [Figure 1-31](#) shows an ATX motherboard.



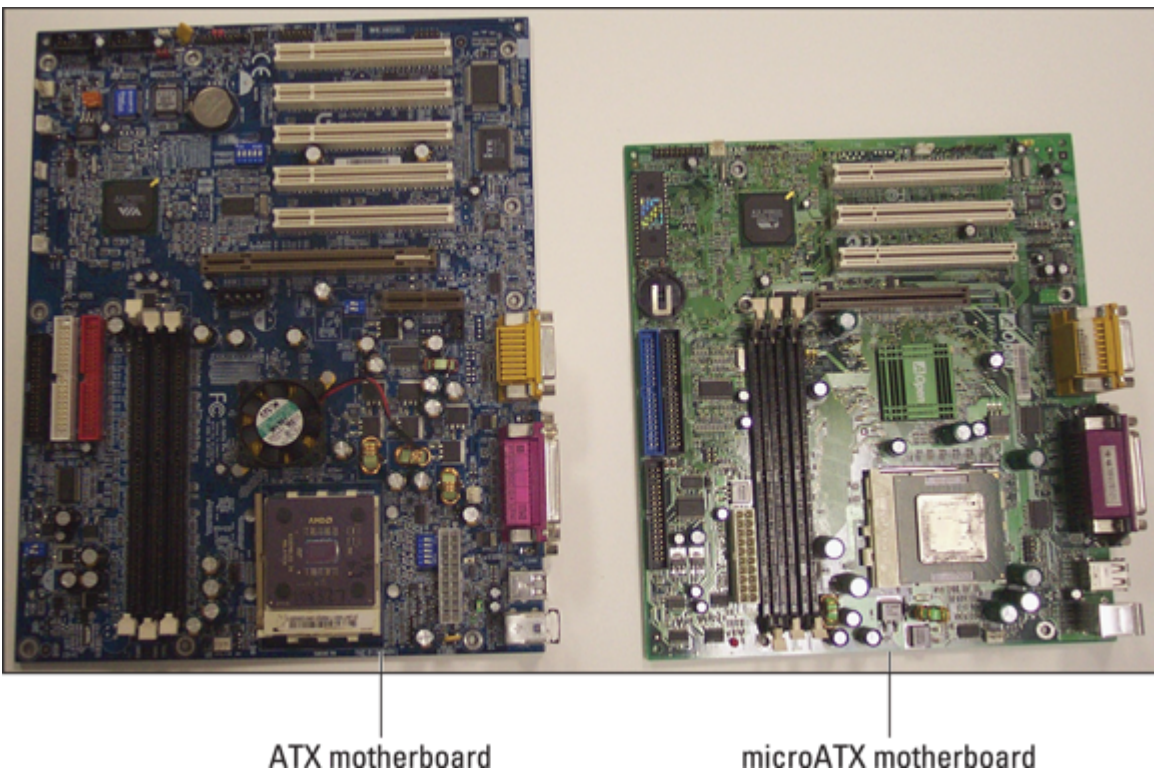
**FIGURE 1-31:** The ATX motherboard is very popular in today's systems.

[Figure 1-31](#) also highlights some of the common components on the ATX board. Notice, for instance, slot 1, where the older Pentium II processor chip was inserted. Newer versions of the ATX motherboard use a ZIF socket to house the processor. Notice also, in the top-right corner, the BIOS chip with a white label on top of it. At the top of the figure, you can identify the EISA and PCI slots, and located in the center of the board is an AGP slot. The hard drive connectors are located on the left side beside the three slots that hold the DIMM.



## *microATX and FlexATX*

Smaller versions of the ATX motherboard are the microATX (also known as mATX) and FlexATX. The microATX motherboard form factor is 9.6 x 9.6 inches and can fit in either a microATX case or a normal ATX case, known as a full ATX case. Measuring 9 x 7.5 inches, the FlexATX is smaller than the microATX but can fit in an ATX or a microATX case. FlexATX is not as popular because the size of the motherboard limits how much you can expand the system. [Figure 1-32](#) shows a microATX board.



**FIGURE 1-32:** Compare ATX motherboard size (left) with a microATX motherboard (right).

The important point to make here is that when you purchase a motherboard, you must ensure that it fits your case. For example, if you have an ATX case, you know that an ATX or microATX motherboard can fit in that case.

## *ITX*

The ITX motherboard form factor was developed by VIA Technologies and comes in different form factors. Each form factor of ITX has different dimensions and is designed to function in different devices:

- » **Mini-ITX/mITX:** A low-power motherboard form factor that is smaller than the microATX with dimensions of 6.7 x 6.7 inches. Because of their low power consumption, they are kept relatively cool and are typically used in home theater PCs. The mini-ITX is also known as the mITX.
- » **Nano-ITX:** The Nano-ITX form factor was developed in 2005 and has dimensions of 4.7 x 4.7 inches. The Nano-ITX form factor is a low-power-consumption form factor as well and is used in devices such as PVRs, media centers, and car PCs.
- » **Mobile-ITX:** The Mobile-ITX form factor (2009) is used for compact devices such as smartphones, with dimensions such as 75mm x 45mm.



FOR THE  
EXAM

Another motherboard form factor that was designed to replace the ATX form factor and create smaller, low-profile systems is the Balanced Technology eXtended (BTX) motherboard form factor.



ON THE  
WEB

Lab 1-3 will help you summarize distinguishing features of popular motherboard form factors. Lab 1-3 can be found on the companion website at [www.dummies.com/go/aplusaio](http://www.dummies.com/go/aplusaio).

## *Understanding Bus Architectures*

The motherboard has a number of expansion slots that can expand the computer's capabilities. When the system is first purchased, a computer has only so many capabilities. The nice thing is that you can expand on those capabilities by purchasing cards to add to the expansion slots, or bus slots.

*Expansion slots*, um, expand what the computer can do. The problem is that there are different types of expansion slots in the system, so when you

purchase a sound card or network card, you have to make sure you get the right type. In the following sections, I show you the different types of expansion slots and also compare their characteristics.



**REMEMBER** Another term for the expansion slots is *bus slots*. A number of different bus architectures have been developed over time. You need to be able to identify the differences between each of these architectures and also to know which ones are more popular today.

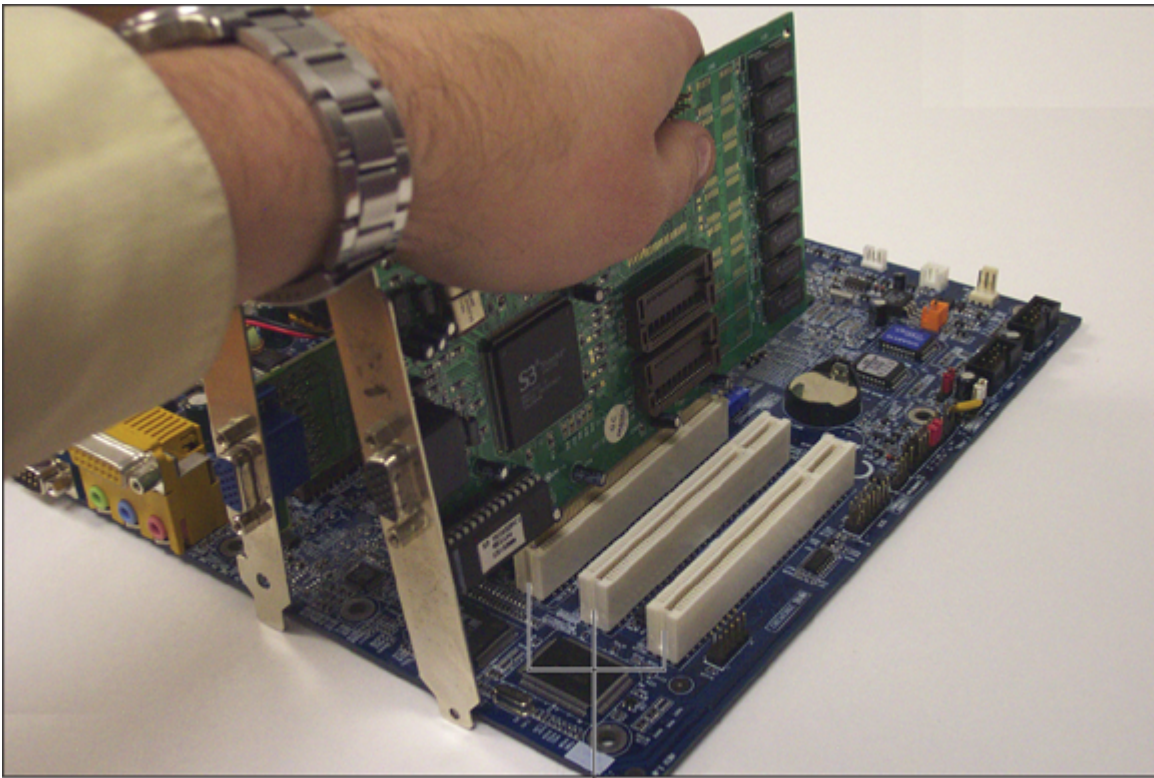
## **PCI**

Peripheral Component Interconnect (PCI) has two flavors: 32-bit cards and 64-bit cards. When Pentium systems hit the market, their motherboards featured both ISA/EISA slots and PCI slots. When buying a new card today, you would most likely buy a PCI device for one of the PCI slots in your system.

The 32-bit version of PCI has a speed of 33 MHz with a transfer rate of 133 MBps, and the 64-bit version of PCI runs at 66 MHz. PCI also supports bus mastering. One of the other major benefits of PCI is that it is a Plug and Play architecture. If you are running a Plug and Play operating system, such as Windows, and your computer has a Plug and Play BIOS, the system resources (such as IRQs and I/O addresses) are dynamically assigned for PCI components.

PCI slots are easily identified on the motherboard as the small white slots, usually located alongside the AGP slot. [Figure 1-33](#) identifies PCI slots on a motherboard.





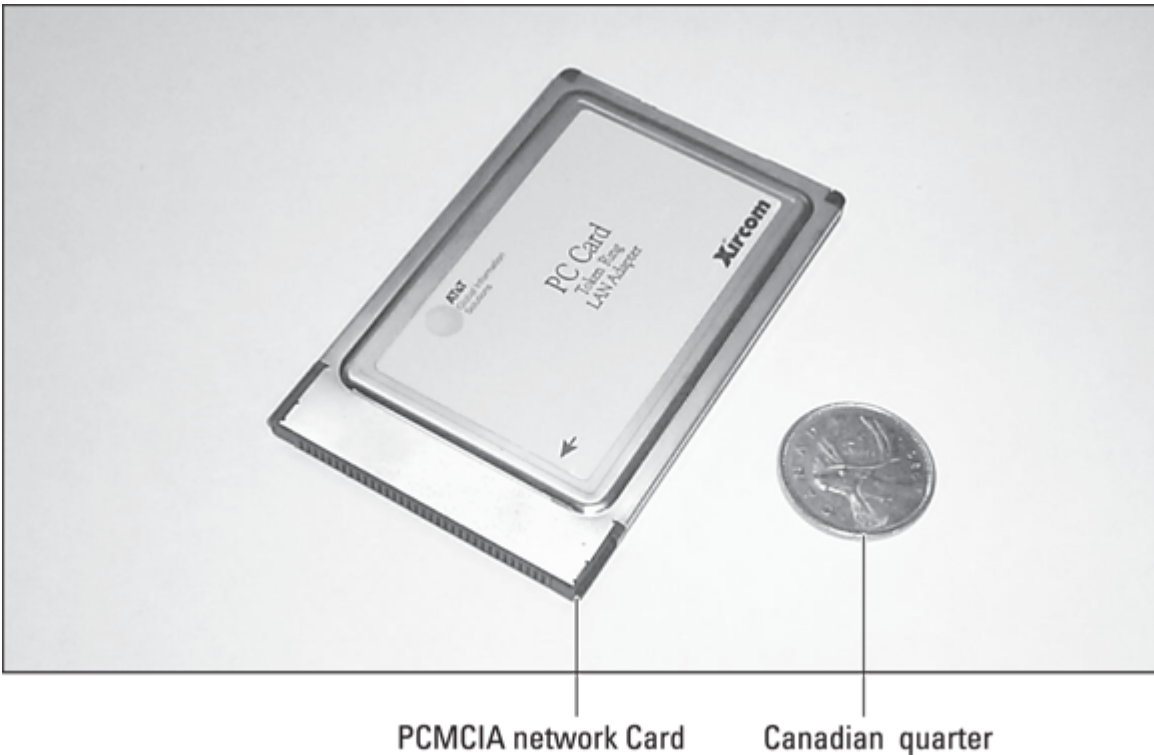
PCI slots

**FIGURE 1-33:** Installing a card into a PCI slot on a motherboard.

## *PCMCIA*

*Personal Computer Memory Card Industry Association (PCMCIA)* is a unique type of expansion bus architecture because of its small size.

PCMCIA is popular in laptop computers. After all, how can you get a big network card like the one in a desktop computer into a little laptop to add network support? The answer is that you can't; you have to purchase a PCMCIA network card for the laptop to add network support. *PCMCIA cards*, also known as *PC Cards*, are a little bit larger than a credit card and can fit into your back pocket (although I don't suggest that you put one there). [Figure 1-34](#) shows a PCMCIA network card.



**FIGURE 1-34:** A PCMCIA network card.

PCMCIA (say that five times fast!) is a 16-bit architecture that runs at 33 MHz, supports Plug and Play, and is also a *hot-swappable* technology. That is, you can insert and remove PCMCIA cards without first shutting down the system. PCMCIA has three different types of slots: type 1, type 2, and type 3.

[Table 1-1](#) shows the different PCMCIA slot types and the types of devices you can find in the different types of slots.

**TABLE 1-1 PCMCIA Slot Types**

Slot Name	Thickness	Types of Devices
Type 1	3.3mm	Memory cards
Type 2	5.0mm	Modems/network cards
Type 3	10.5mm	Removable drives

Type 1 cards were originally used to add memory to laptop computers or personal computers. This is where the “personal computer memory card”

part of the PCMCIA name comes from.

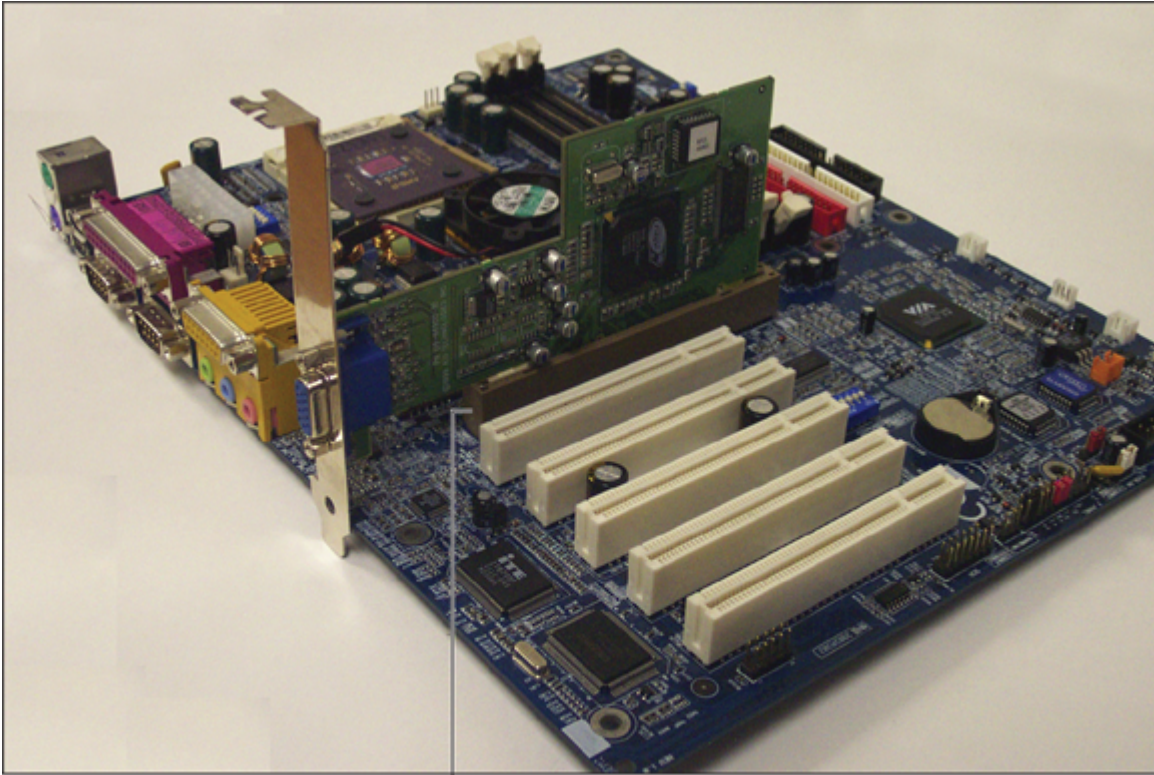


FOR THE  
EXAM

PCI is a 32- or 64-bit technology, runs at 33 MHz, and supports Plug and Play. PCMCIA is an older expansion bus architecture used by laptop computers and is a 16-bit architecture that runs at 33 MHz.

## **AGP**

*Advanced Graphics Port (AGP)* has been around since the Pentium II processor appeared in 1997. It's a 32-bit bus architecture that runs at 66 MHz, which is twice the speed of the PCI bus. Many older motherboards have one AGP slot to hold an AGP video card. The performance gain from the AGP port comes not only from the increase in speed, but also because the AGP bus has a direct path to the processor so that information travels quickly from the processor to the AGP card. [Figure 1-35](#) shows an AGP slot beside some PCI slots.



AGP slot

**FIGURE 1-35:** An AGP card in an AGP slot.

AGP can run in different modes; each mode runs at 66 MHz but has a different transfer rate on the bus. AGP 1x mode has a transfer rate of 266 MBps, AGP 2x has a transfer rate of 533 MBps, AGP 4x has a transfer rate of 1.07 GBps, and AGP 8x has a transfer rate of 2.2 GBps!

## ***PCI-X***

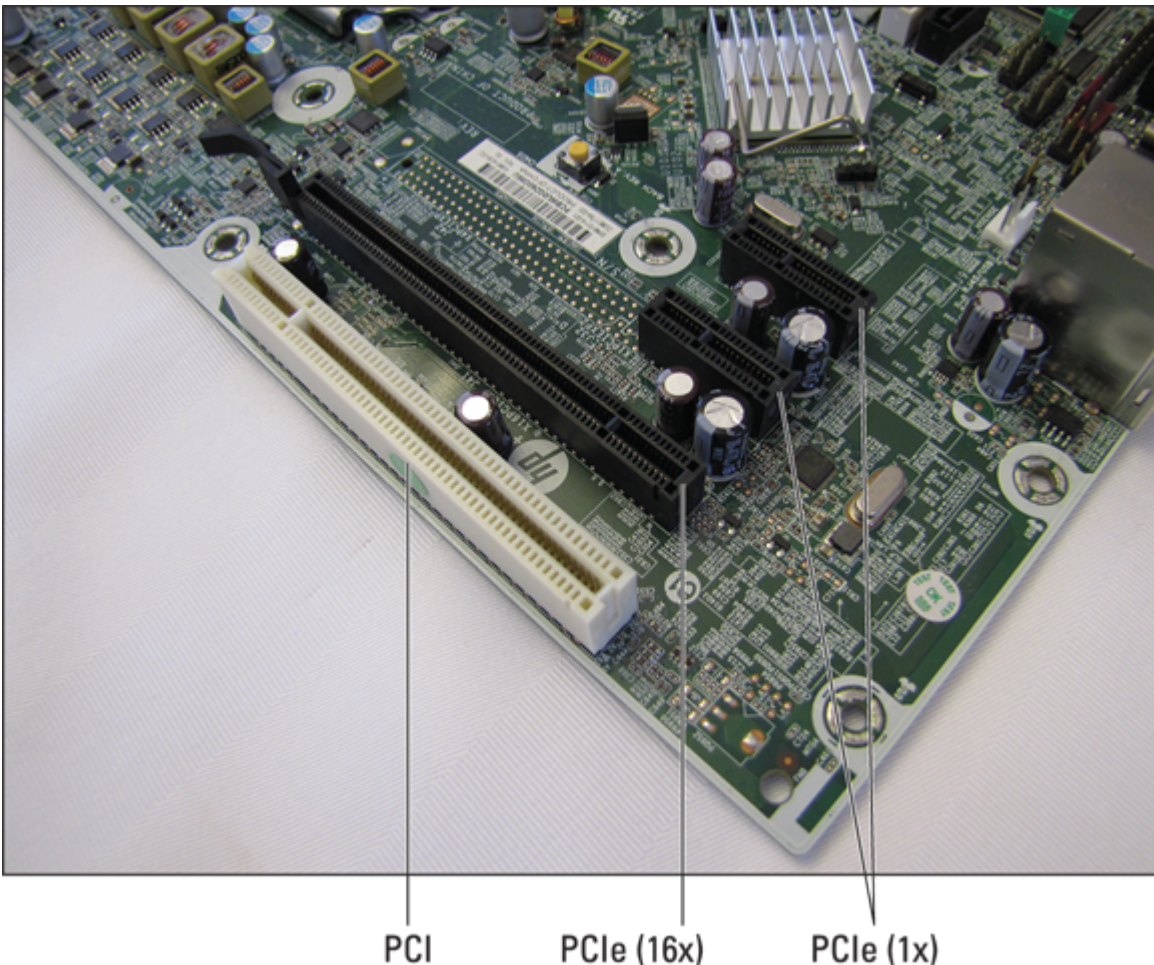
One bus architecture to arise on the market after AGP is the Peripheral Component Interconnect Extended (PCI-X) bus architecture. Because PCI-X uses the same connector style as PCI, it is totally compatible with PCI in the sense that it can hold PCI cards. So, a motherboard with PCI-X slots can also house older PCI cards — and that is a great feature!

Like PCI, PCI-X is a 32-bit and 64-bit bus architecture and is available in four different speeds: 66 MHz, 133 MHz, 266 MHz, and 533 MHz. It is important to note that PCI-X was largely a server bus architecture.

## ***PCI Express***



PCI-X is compatible with PCI by being able to hold PCI cards and also sending data in parallel (multiple bits at one time), but the *PCI Express* (PCIe) bus architecture takes a totally different approach. PCIe is a serial bus that does not support existing PCI cards. The PCIe slots (1x and 16x), shown in [Figure 1-36](#), are a different size than the PCI slot, so they can't possibly house a PCI card.



**FIGURE 1-36:** PCI Express slots on a motherboard.

PCIe uses data lanes to transfer the information within the bus architecture. A data lane delivers an amazing transfer rate of 250 MBps per lane. PCIe has different implementations, each of which has a different number of lanes identified by a multiplier. For example, PCIe with only one lane is known as x1, and a PCIe bus with eight lanes is known as x8. PCIe can thus reach fast transfer rates by implementing additional lanes. For example, current graphics cards for PCI Express

have 16 lanes that provide a transfer rate of 4 GBps (16 x 250 MBps) — which is twice the rate of AGP 8x, which runs at 2 GBps.

Most motherboards today have a combination of PCI and PCI Express slots. You can find systems with PCI Express at x1, x2, x4, x8, x16, and x32. The PCI Express slot gets bigger with each multiplier. For example, [Figure 1-36](#) shows a PCIe 1x slot and the PCIe 16x slot.

## ***AMR and CNR***

*Audio/Modem Riser (AMR)* is a newer bus architecture that adds a modem and audio card to the system. AMR allows the two components to be incorporated into a single card to reduce cost.

*Communication and Network Riser (CNR)* is another bus architecture that has come out in recent years, used to implement LAN, audio, and modem functionality all in one.

## ***miniPCI and miniPCI Express***

Laptop computers also have expansion buses, but they obviously must take smaller cards. Those smaller cards are miniPCI or miniPCI Express (also known as miniPCIe). miniPCI is a 32-bit architecture that runs at 33 MHz, while miniPCIe is a serial technology like PCIe.



**FOR THE  
EXAM**

As far as the “real world” and the A+ exams are concerned, you need to be extremely strong in the area of bus architectures. A big part of servicing computers is installing network cards, sound cards, and video cards. These components come as PCI, PCI Express, or AGP cards today. You need to know how to look at a system and say, “We are going to buy a PCI network card for this system.”



**ON THE  
WEB**

Lab 1-4 will help you identify the different performance characteristics of each of the standard bus architectures. Lab 1-4 can

be found on the companion website at  
[www.dummies.com/go/aplusaio](http://www.dummies.com/go/aplusaio).

## *Types of expansion cards*

Now that you have read about the different types of expansion slots that can exist on a computer, let's take a look at the common types of cards you would install in these expansion slots.

- » **Video cards:** Your system will likely have a video card built into the motherboard — this is known as an *onboard video card*. The onboard video card is great for the typical home user who is using the computer for surfing the Internet, word processing, or spreadsheet work. A person into gaming may need to purchase an *add-on card* (video card) that has more memory and a GPU that can handle the complex computations required by the video games.
- » **Sound cards:** Someone requiring more intense audio processing may have to purchase a sound card and install it into the system. The built-in audio ports are great for the typical user, but someone requiring more audio power may need to install a sound card.
- » **Network interface card:** Most motherboards today come with a 1 Gbps network card. If you are installing a server operating system or firewall on the computer, you may decide to add network cards to the system by installing additional NIC cards.
- » **USB expansion card:** If you require additional USB ports you may need to install a USB expansion card that would give you additional USB ports out the back of the computer.
- » **eSATA card:** If you are connecting eSATA drives to the system and your computer did not come with an eSATA port, you will need to install a card that gives you eSATA ports.

## *Performance Considerations*

When you want to improve a motherboard's performance, one of the first things you should do is check the motherboard speed. For example, some

systems today have 600–1500 MHz motherboards. To find out the speed of the motherboard, check the board documentation. You can get a performance increase from a faster motherboard.

Another performance consideration occurs when you add expansion cards to the system. You should first evaluate what expansion slots are free and then purchase a card that will give you the best performance. For example, when you need to buy a network card, start by looking at what expansion slots are free. If only two slots are free — say, a PCI slot and a PCIe slot — your choices are then obviously limited to a PCI network card or a PCIe network card. In this case, you would want the PCIe slot for video cards because it outperforms PCI as a technology, which means you may use the PCI for the network card. If you have multiple PCIe slots free then maybe look to a PCIe network card.

You can also get a performance increase from motherboards that have more cache memory. Look at the motherboard to see whether there is a place to install some Level 2 (L2) cache. L2 cache can dramatically increase performance because it is generally closer to the processor than the system memory (RAM) and is a faster type of memory than the system memory. Bottom line: The more cache memory you install, the better the motherboard's performance.

## Getting an A+

This chapter introduces you to a number of key components of the motherboard and different motherboard form factors. The following is a list of the key points to remember when dealing with motherboards:

- » The *motherboard* (or *system board*) is the computer component that interconnects all other components.
- » Serial (COM) ports come in two flavors: DB9-male and DB25-male. Parallel ports come in only a DB25-female port.
- » The two main types of cache memory are L1 and L2 cache. L1 cache memory is integrated into the processor, and L2 cache is contained



outside the processor but in the processor casing or on the motherboard.

- » IDE and EIDE are older hard drive interfaces used to connect hard drives to the system. IDE supports two devices in the IDE chain, whereas EIDE has two channels with two devices in each channel (a total of four devices).
- » SATA is the newer and more common technology to connect hard drives to the system. Each SATA drive has a direct connection to the motherboard and supports hot swapping.
- » A number of major motherboard form factors are available, such as NLX and ATX. Motherboard form factors differ in the size of the board and the layout of the components stored on the board.
- » You may add components, such as a sound card or network card, to the computer by inserting an expansion card into one of the expansion slots in the system.
- » AGP and PCI Express are the common bus architectures used to insert a video card in today's systems.
- » You may increase the performance of the system by using a faster motherboard or by purchasing better-performing expansion cards.

## *Prep Test*

- 1. PCIe expansion cards are made up of multiple lanes labeled x1, x8, or x16. What is the transfer rate of each lane?**
  - (A) 480 MBps
  - (B) 250 MBps
  - (C) 1 GBps
  - (D) 12 MBps
- 2. Which bus architecture supports 32-bit/64-bit cards and transfers information at 33 MHz?**
  - (A) ISA

- (B) EISA
- (C) AGP
- (D) PCI

**3. Which motherboard component is responsible for charging the CMOS RAM so that CMOS can maintain its data?**

- (A) Battery
- (B) BIOS chip
- (C) CMOS chip
- (D) Power supply

**4. You are a consultant and have been asked by your customer what the function of the North Bridge chip is. Which of the following would you say to the customer?**

- (A) The North Bridge chip controls communication from the processor to the USB.
- (B) The North Bridge chip controls communication from the processor to faster technologies such as memory, AGP, and PCIe.
- (C) The North Bridge chip controls communication from the processor to the PCI.
- (D) The North Bridge chip controls communication from the processor to the IDE drive.

**5. You are troubleshooting the startup of a system that seems to need you to enter the date and time every time the system boots up. What should you do?**

- (A) Ensure memory modules are seated properly
- (B) Ensure the video card is seated properly
- (C) Replace the CMOS battery
- (D) Flash the BIOS

**6. How many devices are supported in a USB chain?**

- (A) 10
- (B) 27
- (C) 127
- (D) 255

**7. Your manager has asked you to explore external hard drive technologies to use that would give the best performance. Which of the following would you recommend?**

- (A) IEEE 1394a
- (B) USB 3.0
- (C) IEEE 1394b
- (D) S1600

**8. You are the lead consultant at your company. Your customer is looking to improve the performance of one of the video editing systems by installing a new graphics card. Which of the following video cards would be the better performing video card to purchase?**

- (A) PCI
- (B) PCIe x16
- (C) AGP x8

**9. What type of cache memory was originally found on the motherboard and is now integrated into the processor?**

- (A) L1
- (B) L2
- (C) SDRAM
- (D) SRAM

**10. Your motherboard includes SATA 2.0 and SATA 3.0 ports. You connect a drive to the SATA 3.0 port. What is the transfer rate to and from that drive?**

- (A) 480 Mbps

- (B) 3 Gbps
- (C) 1.5 Gbps
- (D) 6 Gbps

**11. What is the bus architecture used with laptop computers?**

- (A) PCI
- (B) PCMCIA
- (C) PCIx
- (D) AGP

**12. Your office has some older Pentium class systems that contain AGP slots. Your manager asks about the benefit of AGP. How would you respond?**

- (A) AGP slots have a direct path to the processor to help increase performance of AGP devices.
- (B) AGP cards run at 33 MHz.
- (C) AGP runs at 66 MHz and gets access to the processor through the PCI bus.
- (D) AGP stands for Advanced Graphics Port and is used to install additional video memory.

**13. You have an older laptop that requires a modem so that the user can dial into the company network and access files while he is on the road. Which PCMCIA card type is used for modems?**

- (A) Type I
- (B) Type II
- (C) Type III
- (D) Type IV

**14. You wish to create a dial-in server out of your Windows desktop machine. You purchase an external modem in order to connect it to the desktop computer. Which port is typically used for a modem?**

- (A) USB
  - (B) LPT1
  - (C) COM1
  - (D) LPT2
- 15. You are a consultant and have a customer looking to install a few hard drives in one of their high-end desktops. Which of the following are used to connect internal hard drives?**
- (A) USB
  - (B) SATA
  - (C) IEEE 1394
  - (D) eSATA
- 16. Your customer has asked you to build a custom computer out of a few of the old components she has in the server room. You are handed an ATX case to start with. Which of the following motherboards will fit in the ATX case? (Select two.)**
- (A) Ultra ATX
  - (B) ATX
  - (C) IPX
  - (D) NLX
  - (E) Micro ATX

## *Answers*

1. **B.** Each lane in a PCIe expansion card is 250 MBps. See “[PCI Express](#).”
2. **D.** The PCI bus architecture is a 32-bit and 64-bit architecture that runs at 33 MHz. AGP runs at 66 MHz. Review “[PCI](#).”
3. **A.** The battery is responsible for maintaining a charge so that the CMOS RAM doesn’t lose its information. The BIOS chip stores the

core system code that allows all the devices to communicate. *Check out “[CMOS battery](#).”*

4. **B.** The North Bridge chip controls communication to high-speed buses such as memory, AGP, and PCIe, while the South Bridge chip handles communication to slower technologies such as USB, PCI, and legacy hardware. *Peruse “[Motherboard chipset](#).”*
5. **C.** When you boot a computer that prompts for the date and time, this is a great indication that the computer is forgetting the information stored in CMOS. This is most likely due to the battery needing to be replaced on the motherboard. *Take a look at “[CMOS battery](#).”*
6. **C.** A computer can support up to 127 USB devices in a USB chain. *Peek at “[USB ports and the internal USB connectors](#).”*
7. **B.** USB 3.0 has a transfer rate of 5 Gbps, while 1394a has a transfer rate of 400 Mbps, IEEE 1394b has a transfer rate of 800 Mbps, and S1600 runs at 1.57 Gbps. *Look over “[USB ports and the internal USB connectors](#).”*
8. **B.** PCIe is the newer bus architecture that has the better transfer rates and should be used if PCIe slots are available. PCIe in this case has a transfer rate of 4 GBps (16 x 250 MBps), while AGP 8x would have a transfer rate of 2 GBps. *Study “[PCI Express](#).”*
9. **B.** Level 2 (L2) cache is the type of cache memory that is found on motherboards, whereas Level 1 (L1) cache is found in the processor. Choices C and D are not types of cache memory. *Refer to “[Cache memory](#).”*
10. **D.** SATA 3.0 has a transfer rate of 6 Gbps, while SATA 2.0 has a transfer rate of 3 Gbps. SATA 1.0 has a transfer rate of 1.5 Gbps, while USB 2.0 has a transfer rate of 480 Mbps. *Examine “[SATA connections](#).”*
11. **B.** The bus architecture used in laptop computers is called PCMCIA (Personal Computer Memory Card Industry Association). The other three choices are bus architectures available to desktop computers. *Review “[PCMCIA](#).”*

12. **A.** The AGP slot runs at 66 MHz and has a direct path between the slot and the processor so that information will not have to travel through one of the slower buses. AGP stands for Advanced Graphics Port and is used to install a video card, not video memory. *Check out “[AGP](#).”*
13. **B.** Type II cards are used for network cards and modems. Type I cards are used for memory upgrades, and Type III cards are used for removable drives. *Peruse “[PCMCIA](#).”*
14. **C.** COM1 is a serial port that is typically used for modems or serial mice. LPT ports are parallel ports that are generally used to connect printers. *Take a look at “[Serial ports](#).”*
15. **B.** Computers today use SATA drives as internal drives for computers. The SATA drive connects to the SATA port located on the motherboard. *Look over “[SATA connections](#).”*
16. **B and E.** An ATX case can hold an ATX motherboard or a Micro ATX motherboard. *Study “[ATX](#).”*

# Chapter 2

## Picking Your Processor

---

### IN THIS CHAPTER

- » Understanding CPU characteristics
  - » Identifying popular CPUs
  - » Identifying sockets
  - » Installing a processor
- 

Although all components of the computer function together as a team, every team needs a leader — someone who gives instructions and keeps everyone working toward the same goal. If any PC component were considered the team leader, it would probably be the *central processing unit (CPU)*, also known as the *processor*. The key word here is *central*, which implies “center” or “focus.” The CPU can be considered the focus of the computer because it controls a large number of the computer system’s capabilities, such as the type of software that can run, the amount of total memory that the computer can recognize, and the speed at which the system will run.

In this chapter, you get a look at some of the features of the CPU that are responsible for regulating the capabilities of the computer system. This chapter also discusses the importance of the CPU and its role as a PC component, and also identifies some of the main characteristics that make one CPU better than another.



**FOR THE  
EXAM**

When preparing for the A+ exams, it is important that you are comfortable with terms like *MMX*, *throttling*, and *cache memory*. You also want to be sure that you are comfortable with the



differences between various processors. For example, what makes an Intel Core i5 better than a Celeron? Which AMD processor competes with the Celeron? All these are questions you should know the answer to before you take the A+ exams, and this chapter helps you find the answers. Good luck!

## *Understanding Processor Terminology*

In this section, I cover some basic terms that describe characteristics of different processors, past and present. The A+ exams might not ask for the specific definition of each term, but understanding the terms will help you answer the related questions in this topic area.

### *Processor speed*

*Processor speed* is how fast a processor executes its instructions or commands. This speed was originally measured in millions of hertz, or megahertz (MHz), per second. A *hertz* is also known as a clock cycle, and a processor can execute code at every clock cycle. Thus, a processor operating at a measly 1 MHz per second can execute one million tasks every second. Processors today now measure their speed in gigahertz (GHz) per second. A *gigahertz* is one billion clock cycles per second — so the CPU can execute tasks a billion times per second!

Original CPUs had a speed of 4.77 MHz, and systems at the time of this writing are running over 3.0 GHz. Although processor speed is not the only factor affecting performance, in general, the faster the processor, the faster the system.

### *Data bus*

A city bus is responsible for transferring people from one location to another. In the world of computers, a *bus* is responsible for delivering data from one location on the PC to another. *Data bus* is the term used to define the pathway between the processor and memory. Because the processor accesses information from memory so often, an entire bus —

the data bus — is dedicated to this action. The larger the data bus, the more data can be carried from the CPU to memory in one clock cycle.

Here's an illustration. Say 50 people needed to go from one end of the city to the other, but a city bus had only 25 available seats. The solution? The bus would make two trips. Hmm. Wouldn't getting a larger bus be more efficient? If you upgraded the bus to 50 seats, the bus would have to make only one trip to transfer the 50 people from one end of the city to the other, which increases the efficiency of the public transit system.

The data bus works the same way, only it transfers data in the form of bits. A single bit is either a one or a zero. All data processed by the computer is in the form of bits. The data bus has a full capacity point at which it cannot handle any more bits of data, just like the bus system in the city has a full capacity point (measured in seats).

If a processor has a 32-bit data bus, it can deliver — at most — 32 bits during a single clock cycle. If the same processor needs to deliver 64 bits of information, it has to take two trips: sending 32 bits during the first clock cycle and the remaining 32 bits during the next clock cycle. Taking that same 64 bits of information and processing it on a 64-bit processor means that the information will be delivered in one trip — one clock cycle — as opposed to two, which increases the overall efficiency of the system.

## *Address bus*

[Figure 2-1](#) shows how system memory is organized like a spreadsheet, in rows and columns. These rows and columns make up blocks that can be written to and read from. If you want to store information in one of the blocks, you have to reference the location by address. For example, you may store data in cell B2.

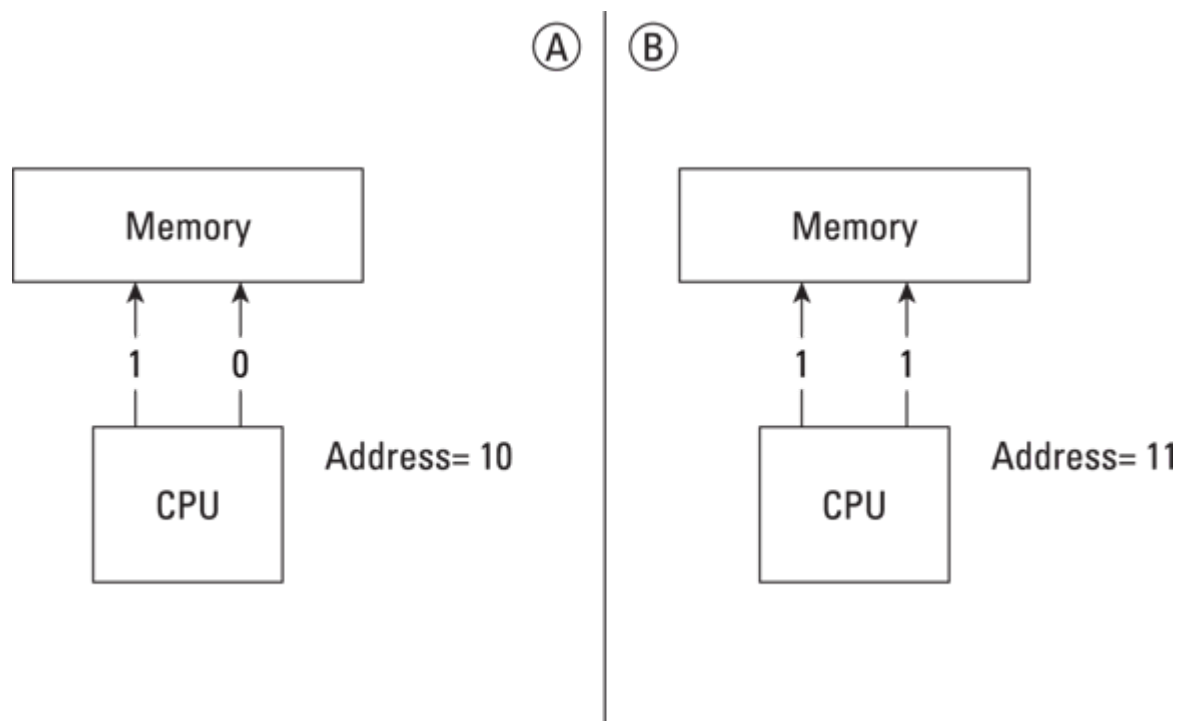
	A	B	C	D
1				
2				
3				
4				
5				

**FIGURE 2-1:** How system memory is organized.

To store information into system memory, your processor has to give an address that points to a particular storage location, only the address doesn't look like B2. It looks something like 10, or maybe 11, which are two completely different memory locations. As a result, the data would get stored in two different blocks.

Your processor accesses memory locations through the *address bus*. If, for example, the address bus is two-bit, the processor has two address lines from the processor to system memory. The *address lines* carry signals that specify locations in memory, each with an on/off state. A 1 represents an on state, and 0 represents an off state. The combination of the on/off states of both address lines at any given time is how a reference to an area in memory is made. The left side of [Figure 2-2](#) illustrates a processor making a reference — or *call* — to address 10. The left side of

the figure shows a reference to address 11. These two address calls reference completely different locations in memory.



**FIGURE 2-2:** Accessing two different memory addresses with the address bus.

If you add another address line to the address bus, the processor can access even more possible addresses because the processor has more variations with three bits than with two. A two-bit address bus can make a reference to four possible memory addresses ( $2 \times 2$ ), but a three-bit address bus can make a reference to eight possible memory addresses ( $2 \times 2 \times 2$ ).

Therefore, the address bus dictates how much physical memory the processor can access. For example, an old 80286 processor has a 24-bit address bus, which means that it can access 16,777,216 ( $2^{24}$ ) memory addresses, or 16MB of system memory. A few years back, some processors had a 36-bit address buses, which allows them to access 68,719,476,736 memory addresses, or 64GB of memory. Newer processors are exceeding the 36-bit address bus, and one more example is a 40-bit address bus which allows for 1,099,511,627,776 addresses (or 1 TB of RAM)!

## *Registers*

*Registers* are storage areas within the processor used to store data temporarily for manipulation later. They are used to store and process data and perhaps write back the result of the processed data. The benefit of storing this information in the registers — instead of in memory — is that the processor contains the information and does not have to retrieve it from memory, which takes time. It is as if information to be processed were in your pocket, rather than across a room, where you would have to walk all the way over and pick it up. Having information in your pocket means it can be accessed much more quickly, saving time and increasing performance. Registers give a processor quicker access to data; the more registers a processor has, the more data it can store.

Registers are measured in bits. A processor with 32-bit registers has 32 containers into which a programmer can choose to store information. Comparatively, a processor with 64-bit registers has twice as many containers that it can use to store information.

## *Cache memory*

The processor accesses information that resides in system memory, which is a slower process than if the information is stored in the processor's own special high-speed memory, known as *cache memory*. When the information is sitting in system memory and the processor sends a request for that information, the request goes to the *memory controller*, which manages data in memory. The memory controller finds the data in memory, retrieves it, and delivers it to the processor. Throughout this entire process, the processor is simply waiting around for the information. Thus, many newer processors include their own special high-speed memory within the processor's chip.

When the processor retrieves information from slower system memory, it then stores it in the high-speed cache in case the processor wants to access the information a second time. The benefit is that the second time the data is needed, it is sitting in the high-speed memory located on the processor chip. The processor does not need to sit around and wait for the

data to come from system memory — again, increasing overall performance.

Cache memory is integrated right into the processor's chip and is made up of *static RAM (SRAM)*. For more information on SRAM check out Book 2, [Chapter 3](#). Cache memory is very expensive because it is much quicker than regular system memory. As a result of this extra memory being integrated into the processor chip, the processor becomes more expensive than a processor that has less or no cache memory.



FOR THE  
EXAM

The three types of cache memory are *Level 1 (L1) cache*, *Level 2 (L2) cache*, and *Level 3 (L3) cache*. L1 cache is built into the processor, whereas L2 cache resides outside the processor. In the past, L2 cache resided on the motherboard, but newer processors have a bit of L1 and L2 cache for each core in the processor and then a shared block of L3 cache for all cores in the processor.

## ***Math co-processor***

The *math co-processor*, also known as the *arithmetic logic unit (ALU)*, is the processor's sidekick. Systems with math co-processors can well outperform systems that do not because the math co-processor takes some of the workload off the CPU. For example, it performs many of the large calculations that applications may require, such as floating point arithmetic. Overall system performance increases because the CPU can focus on logic functions while the math co-processor executes complicated mathematical functions.

If you have large spreadsheets or use large graphics applications, you might find that applications run very poorly or not at all on systems without a math co-processor. If you are running a system that does not have a math co-processor integrated into the CPU, you can add one to the motherboard, or perhaps upgrade the main processor.

In earlier computers, the processor was one chip, and the math co-processor was a separate chip on the motherboard. Today's processors

all have the math co-processor integrated into the CPU, so you will not purchase or add an NPU to the system — or even hear much about a math co-processor.

## *MMX*

After the Pentium was developed, Intel introduced a feature called *MultiMedia eXtensions*, or *MMX*. MMX added 57 new instructions that were built into the processor and told the system how to work with audio, video, and graphics. If these instructions were not built into the processor, the processor would have to retrieve them from somewhere else.

When MMX was developed, both home and business users seemed to be heading toward the world of multimedia, and it made sense to enhance the processor and make it “multimedia aware.” Running any kind of multimedia application on a processor that supports MMX gives you a major performance increase over a processor that doesn’t support MMX technology.

MMX is an old instruction set, but my point with putting this in here is for you to see that processor manufacturers will install instructions into the processor for whatever is a hot technology at the time in order to increase performance when using that technology.

## *Hyperthreading*

Hyperthreading is a feature designed by Intel that was placed in the Pentium processors. *Hyperthreading technology*, or *HTT*, allows a processor to logically act as two different processors by being able to execute simultaneous threads. A *thread* is a part of an application that executes at any given time. For example, when running Microsoft Word, one thread accepts keystrokes, and another thread runs the spell checker while you type. Thus, two parts of the application run at the same time.

For a system to truly be able to take advantage of multithreaded applications, you normally need a system that has multiple processors — one processor to run one thread at a time. With hyperthreading, one processor can run more than one thread at a time, increasing performance by 15 to 30 percent.

## *Single-core versus multicore*

Everything we have discussed so far about processors has assumed we are talking about a single-core processor. That is, a CPU that is made of only one processor with added benefits such as cache memory and features such as hyperthreading. Nowadays we have what is known as a *multicore processor*.

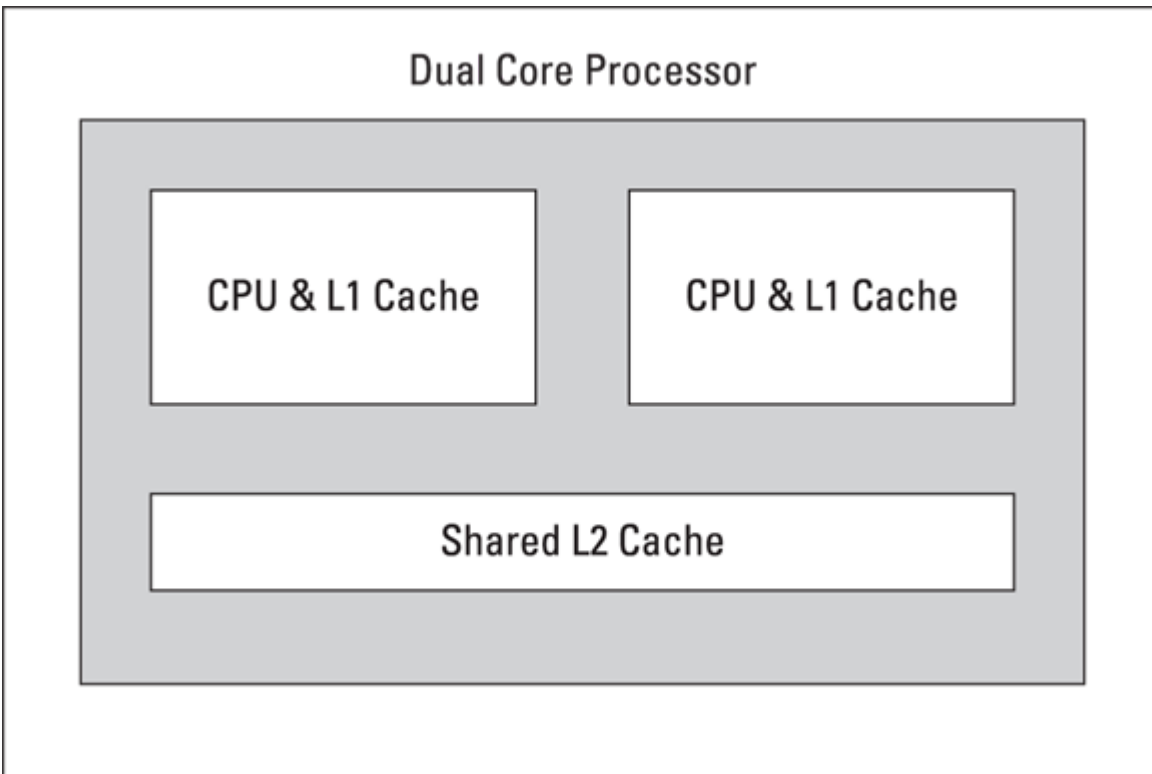
A multicore processor combines a number of independent processors and the L1 cache from those processors onto a single processor chip. The benefit of a multicore processor is that it can execute multiple threads at the same time without hyperthreading because you essentially have multiple processors in one chip package.

A multicore processor has the benefit of having multiple processors' core features — such as superscalar execution, pipelining, and threading — all packaged into one physical processor. The core features also include each core having its own L1 cache memory. Multicore processors also have a block of shared L2 cache between the two processors in the multicore chip.

A huge benefit of being only one chip on the motherboard is that the one multicore chip draws less power than two separate processors would.

[Figure 2-3](#) shows the logical view of a dual-core processor.





**FIGURE 2-3:** Looking at the logical structure of a dual-core processor.

A number of different flavors of multicore processors are available today, such as dual-core, triple-core, and quad-core processors. Here are the differences between the three:

- » **Dual core:** Has two cores in one chip package, with each core typically having 128K of L1 cache and 512K of shared L2 cache.
- » **Triple core:** Has three cores in one chip package with each core typically having 128K of L1 cache. Most triple-core processors also have 512K of L2 cache per core and share a block of cache memory, known as L3 cache.
- » **Quad core:** Has four cores in one chip package with each core typically having 128K of L1 cache. Most quad-core processors also have 512K of L2 cache per core and share a block of L3 cache (2MB–6MB).

## *Virtualization support*

One of the newest features to come from processors in recent years is virtualization support. Virtualization allows you to run multiple computers, known as virtual machines (VMs), on one physical computer. Each virtual machine runs a separate operating system with virtual resources assigned to it such as CPUs, virtual hard drives, and memory.

In order to use virtualization software with your system, your processor must support it and virtualization must be enabled in the BIOS. I don't know how many times I have installed virtualization software such as Hyper-V and then go to start a VM and I receive an error. After this happens, I check the BIOS settings and find out that virtualization support is disabled. A quick change of that setting to "enable" and I am able to run virtual machines!

Depending on the manufacturer of the processor, you will find that the virtualization extensions are called something different. If you have an Intel processor, the virtualization feature is called Intel VT (for *Intel Virtualization Technology*), but if your processor is an AMD processor, then the virtualization feature you must enable is called AMD-V (for *AMD Virtualization*).



FOR THE  
EXAM

To run virtualization software such as Microsoft's Hyper-V, you must have a processor that supports it and it must be enabled in the system BIOS.

## *Architecture (32-bit or 64-bit)*

When purchasing a system, you should always investigate whether the system has a 32-bit processor or a 64-bit processor. The 64-bit processors are needed to run today's 64-bit operating systems and software, and well outperform the 32-bit systems.

Virtualization software — such as Microsoft's Hyper-V — is only available with 64-bit editions of Windows, such as Windows 8.1 or Windows Server. If you do not have a 64-bit computer and a 64-bit edition of Windows 8.1, you are unable to run Hyper-V. My point being if

that was your goal and you did not investigate the architecture of the processor before purchasing the second-hand computer, you may not be able to run the software you want.

## *Integrated GPU*

New processors today may have an integrated graphics processing unit (GPU), which would take care of the video calculations and processing for the system. If the processor does not have an integrated GPU and you need to run heavy graphics applications, you will most likely need to purchase a video card with a dedicated GPU in it.

One of the downfalls of using an integrated GPU is that it will use system RAM as its memory, while a dedicated GPU is an expansion card that has the GPU and its own memory for video processing. This is important because if you have 16GB of RAM in the system and an integrated GPU, the GPU is using some of that 16GB of RAM. A dedicated GPU would not, as it has its own memory on the graphics card.

The benefit of the integrated GPU is that it is less expensive and also uses less power than a dedicated GPU. The integrated GPU would also produce less heat, meaning you wouldn't need to worry about cooling as much.



FOR THE  
EXAM

Remember that the CPU performs *logic* operations, the NPU performs *mathematical* calculations, and the GPU takes care of *video* operations.

## *Execute Disable Bit*

*Execute Disable Bit* (EDB) is a security feature that allows the processor to flag different areas of memory that are, and are not, allowed to run code. This is a great security feature as it is a method to help prevent buffer overflow attacks. *Buffer overflow attacks* are when the hacker submits code to areas of memory in order to run that code. Now with EDB, the code submitted into memory by the hacker would not have

permission to execute unless it is running from an area flagged for code execution.

To take advantage of EDB you must have a processor that supports it, and you must enable it in the BIOS/UEFI.

## Throttling

*Throttling* (a feature built into a lot of newer processors today) involves the CPU sensing when it is going to overheat and then reducing its speed to lower the heat to an acceptable range.

Processors that support throttling have a built-in *thermal sensor* (a high-tech thermometer) that monitors the temperature of the processor. When the processor detects that it is going to overheat — maybe, because of a fan failure — the processor drops its speed so that the temperature drops to an acceptable range.

## Overclocking

*Overclocking*, a big feature for PC enthusiasts, involves running a piece of hardware faster than the speed at which it is rated. A number of devices can be overclocked, such as video adapters and (of course) processors.



**WARNING** Although you might be able to overclock the processor, it is not recommended because overclocking can result in an unstable system or even hardware failure.

## VRM

The *voltage regulator module (VRM)* is responsible for regulating the voltage that is delivered to the processor. The VRM is located on the motherboard (or appears as its own device in the system) and provides the correct running voltage to the processor.

Some VRMs use a jumper on the motherboard to determine how much voltage is supplied to the processor, and other VRMs sense what the

processor needs on startup. Typically, VRMs on the motherboard sense what voltage the processor needs and then supply that voltage.

## ***Chip packaging***

*Chip packaging* refers to how the chip is constructed and delivered to the consumer. The chip package defines the appearance or form factor of the chip. Many chip packages have been used over the years.

The chip packages you should be familiar with for the A+ exams are as follows:

- » **Dual inline package (DIP) chip:** A rectangular chip with two rows of 20 pins. Pin 1 is located at the end of the chip that has a square notch carved into it. It is important to identify pin 1 because when you add a DIP chip to the motherboard, you have to match pin 1 on the chip with pin 1 in the chip socket.

Older processors (such as the 8088) and many math co-processor chips use the DIP chip style. Although they are no longer used for CPUs, DIP chips are still used for cache memory and BIOS chips on motherboards. They are also found on memory modules. (See Book 2, [Chapter 3](#) for a discussion of memory modules.)

- » **Pin grid array (PGA) chip:** One of the most popular processor chip packages in use today, the PGA chip is a square chip with an array of pins filling up the shape of the chip. In general, the PGA chip uses hundreds of pins. You can locate pin 1 on the PGA by identifying the corner of the PGA chip that has the corner cut off — that corner is where pin 1 is located. [Figure 2-4](#) compares a DIP (right side) with a PGA (left side) chip type.

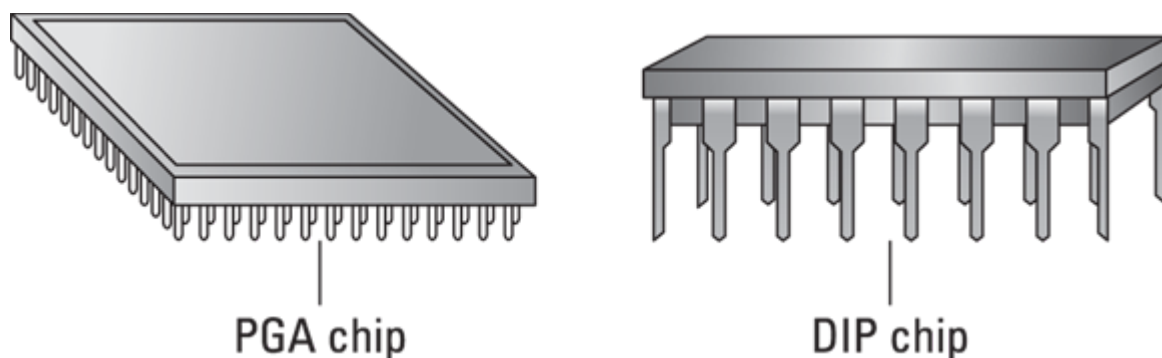
Today's implementations of processors typically fit into a *zero insertion force (ZIF)* socket. The ZIF socket is ideal for upgrading processors (especially compared with the days before ZIF sockets were used) because the ZIF socket has a lever (on the side of the socket) that you lift to raise the chip from the socket. Because the chip is automatically raised out of the socket, you can simply remove the chip out of the socket with little effort!

Before ZIF sockets were used, you had to pry the chip out of the socket while trying to ensure that you did not damage the chip or the pins. With the ZIF socket, after the processor is raised, you can replace the old chip with a new one. In the past, not all boards used ZIF sockets, so you had to get some special extractors to pull the chip out (carefully!). A ZIF socket is shown in [Figure 2-5](#).

- » **Land grid array (LGA) chip:** A chip packaging style similar to PGA is the LGA, which has a rectangular packaging style and contacts instead of pins on the bottom side of the chip. These contacts make a connection to the contacts within the LGA socket on the motherboard when the processor is placed in the LGA socket. An LGA chip and an LGA socket are shown in [Figure 2-6](#).

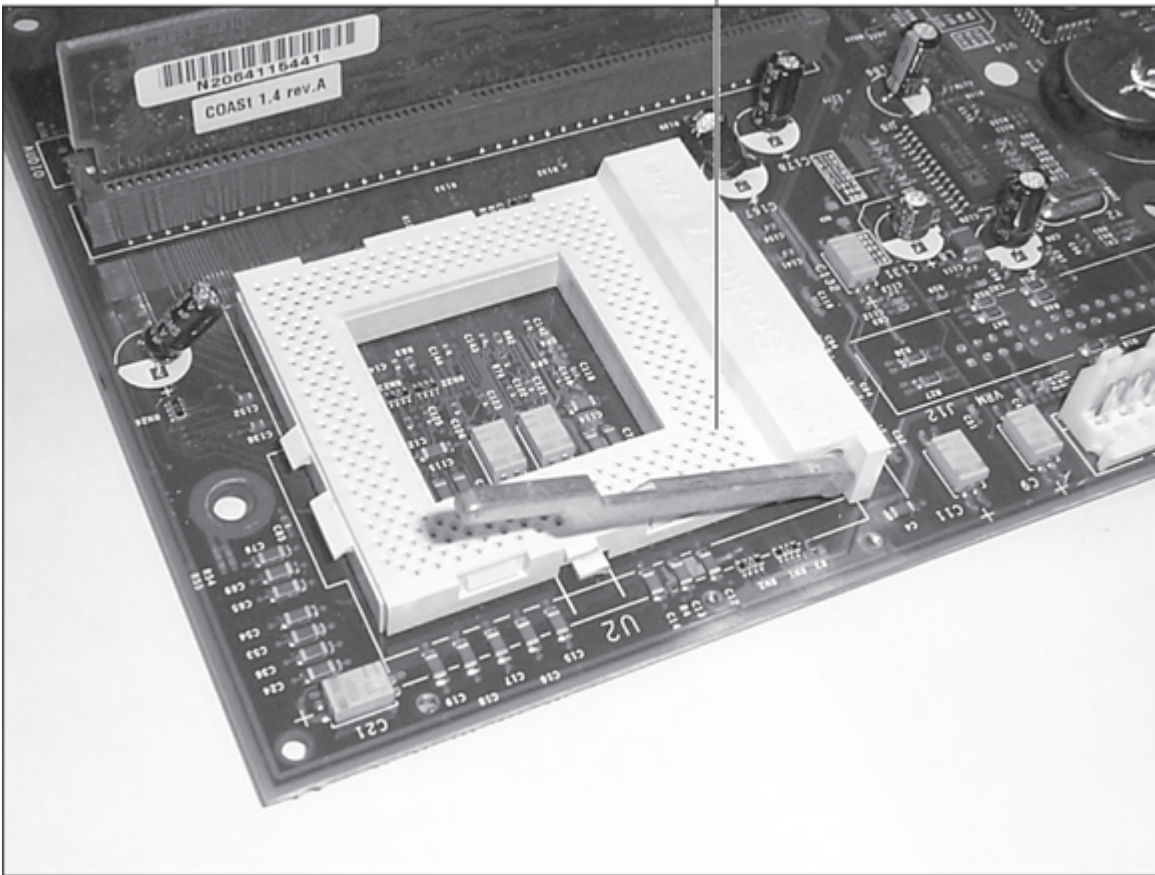
The LGA socket is similar to a ZIF socket in the sense that it is designed to make it easy for someone to remove the processor from the system. The LGA socket uses a surface plate to hold the chip in place.

- » **Single Edge Contact (SEC) chip:** A chip package type that was popular with the Pentium II processors, the SEC chip is a huge cartridge surrounded by a plastic casing. The newer version, SEC2, is implemented as a card that is inserted into a slot on the motherboard and doesn't have the big plastic casing around it. It is important to stress that the SEC and SEC2 are inserted into a slot and not a socket. For more information on slots and sockets, read the next section. [Figure 2-7](#) shows an SEC chip package along with some PGA chip packages.



**FIGURE 2-4:** Comparing a DIP chip package (right) to a PGA package (left).

Socket 7 ZIF socket

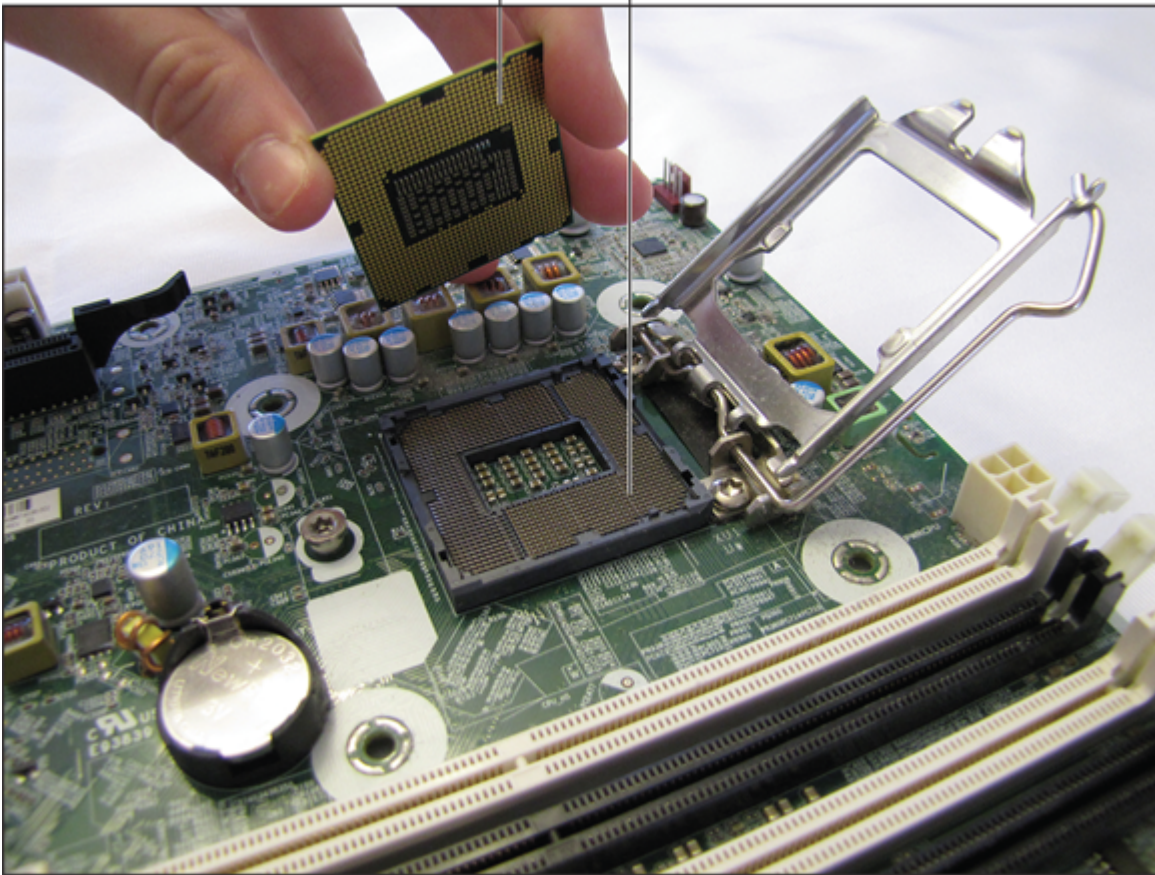


**FIGURE 2-5:** A ZIF socket on the motherboard holds a processor.



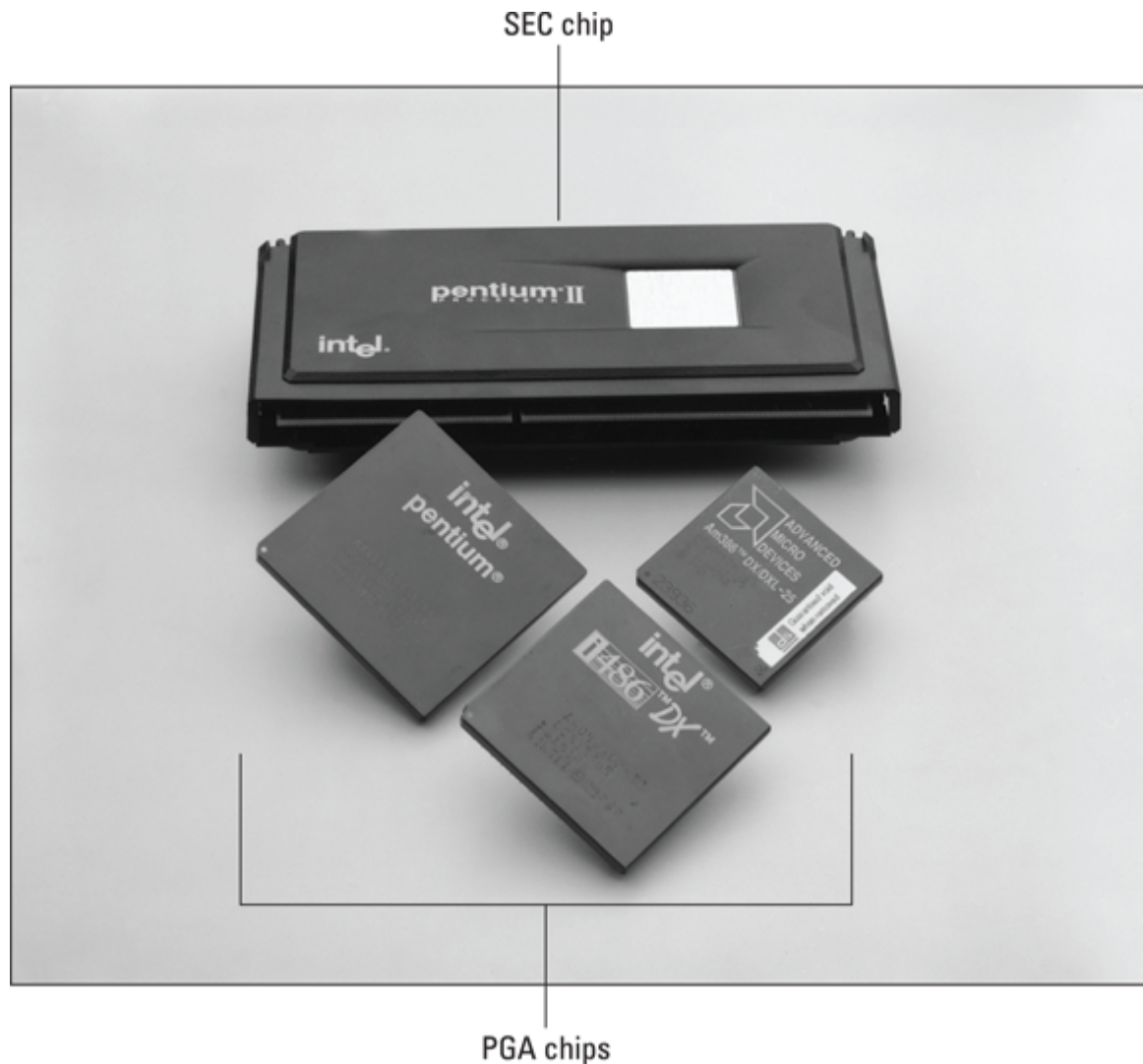
Intel Core i5 processor

LGA socket (socket 1155)



**FIGURE 2-6:** Intel processor and LGA socket.





**FIGURE 2-7:** An SEC chip package along with some PGA chip packages.



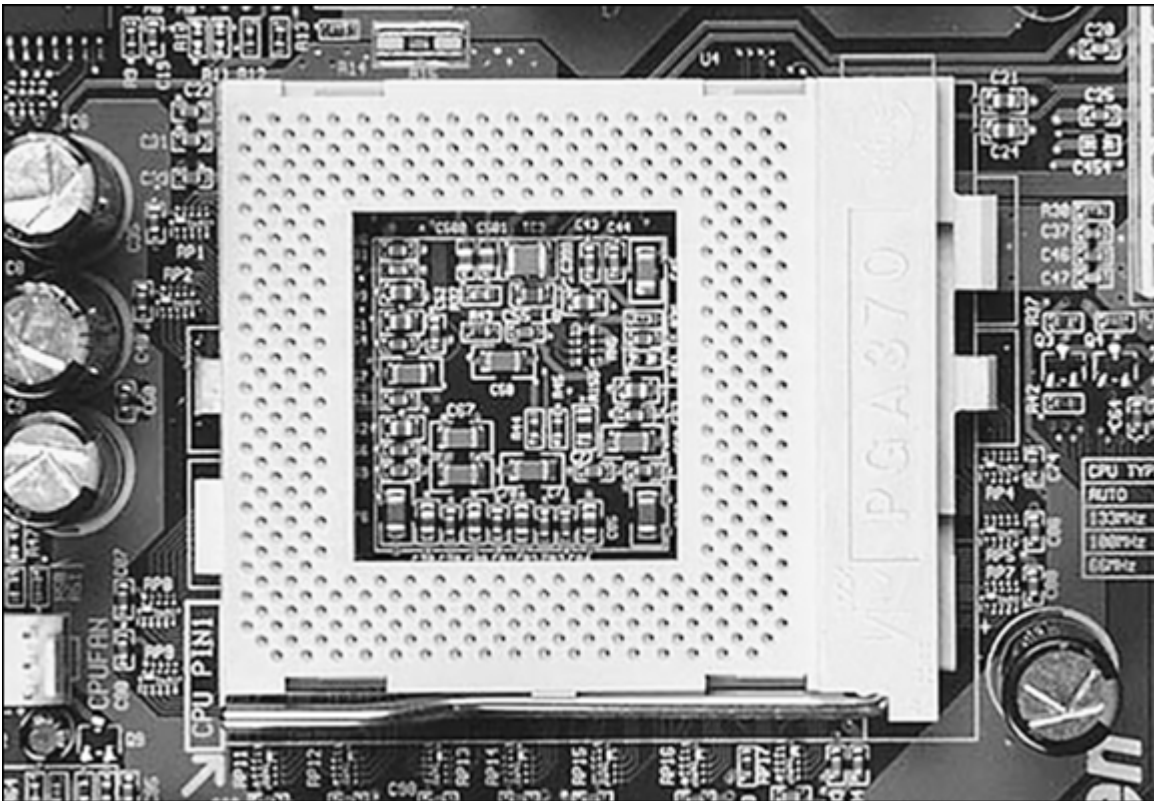
**FOR THE  
EXAM**

Be sure to remember the different chip package types for the A+ exams. The older Pentium II processor used the SEC, while newer processors, such as the Pentium 4 and Intel Core i7 series, are using the PGA and LGA.

## *Identifying Socket Types*

Intel decided to develop a new standard for upgrading a processor on motherboards, beginning with the 80486 chips and continuing with the Pentium-class processors. This standard — a processor socket designed to hold a specific processor chip with the appropriate number of pins — enabled Intel to develop new chips with compatibility of a particular socket in mind. For example, if a socket is developed with 321 pins, Intel could develop a new processor that has 321 pins and know that the processor will work with any motherboard that has the right socket. This allows the consumer to upgrade a processor much easier than in the past. Intel could design a new chip for an old socket so that customers could update their computers by dropping the new processor in the compatible socket.

Original Pentium processors supported mainly Socket 5 with 320 pins or Socket 7 with 321 pins. Thus, to add a Pentium processor to a motherboard, you determine what socket exists on that board and then purchase a CPU to fit in that socket. You also have to remember to match the voltage of the board to the voltage required by the CPU. [Figure 2-8](#) helps you identify a CPU socket in your system.



**FIGURE 2-8:** Identifying a processor socket.

Sockets are normally labeled by type along the side of the socket. For example, in [Figure 2-8](#), the socket is labeled as PGA 370, meaning that it is Socket 370 and will hold any processor designed for Socket 370. (Socket 370 is a socket that holds a processor containing 370 pins.)

[Table 2-1](#) lists the different types of sockets and the processors that are placed in the sockets. For more information about the processors, read the sections “[Looking at Intel Processors](#)” and “[Don’t Forget Non-Intel Chips](#),” later in this chapter. [Table 2-1](#) also shows the number of pins associated with the different types of sockets and slots.

**[TABLE 2-1](#) Processor Socket Types and Slots**

<i>Socket</i>	<i>Processor</i>	<i>Number of Pins</i>
Socket A	Later Athlon, Duron, and Athlon XP	462
Socket 4	Pentium 60/66	273

<b>Socket</b>	<b>Processor</b>	<b>Number of Pins</b>
Socket 5	Pentium 75-133	320
Socket 7	Pentium 75-200	321
Socket 8	Pentium Pro	387
Socket 370	Celeron and Pentium III	370
Socket 418	Itanium	418
Socket 423	Pentium 4	423
Socket 478	Later Celerons and Pentium 4	478
Socket 603	Xeon (Pentium 4 version)	603
Socket 611	Itanium	611
Socket 940	Opteron	940
Slot A	Athlon	242
Slot 1	Pentium II and Pentium III	242
Slot 2	Xeon	330
Socket 754	Turion 64, Athlon 64, Sempron	754
Socket 775 or LGA775 (also called Socket T)	Pentium 4, Pentium D, Celeron D, Core 2 Duo	775
LGA1366 (a.k.a. Socket B)	Intel Core i7 processor	1366
Socket 1156 (LGA)	Intel Core i3, Core i5, and Core i7 – 1st Generation (Lynnfield/Clarksdale)	1156
Socket 1155 (LGA)	Intel Core i3, Core i5, Core i7 – 2nd and 3rd Generation (SandyBridge and Ivy Bridge)	1155
Socket 1150 (LGA)	Intel Core i3, Core i5, Core i7 – 4th Generation (Haswell-DT)	1150
LGA 2011 (a.k.a. Socket R)	Intel Core i7 processor (high-end workstations and servers)	2011
AM2	Opteron, Sempron, Athlon 64, Athlon 64 X2	940
AM2+	Athlon 64, Athlon 64 X2, Phenom, Phenom II	940
AM3	Phenom II	941
AM3+	AMD FX	942

<b>Socket</b>	<b>Processor</b>	<b>Number of Pins</b>
FM1	AMD Llano	905
FM2	Athlon X2 and Athlon X4	904
FM2+	AMD Kaveri APU	906
F	AMD Athlon 64 FX, Opteron	1207



**FOR THE  
EXAM**

Know the socket types used to hold the Pentium 4, Celeron, Intel Core i7, Athlon XP, Athlon 64, Phenom, and Turion processors. You will not be expected to memorize the entire [Table 2-1](#), but you should be familiar with the sockets used by today's popular processors.

Originally, the sockets were simply called Socket 1, Socket 2, and so on up to Socket 8. To make it easier to understand what processors went into which sockets, Intel started naming the sockets after the number of pins that existed on the processor that the socket would support. For example, Socket 370 holds a processor with 370 pins, and Socket 478 holds a processor with 478 pins. It is much easier now to identify what processors go into which sockets!

Now that you understand some of the characteristics of processors and you understand what a socket is, take a look at some of the popular Intel and AMD chips you are expected to know for the A+ exams.

## *Looking at Intel Processors*

In this section, I provide an overview of the Pentium-class processors and their characteristics, including data bus, address bus, registers, and the amount of cache memory supported on these processors. You also are introduced to any new or unique processor features that each processor offers.

## *Pentium*

The original Pentium processor, released in 1993, was developed at speeds of 60 MHz and 66 MHz. The Pentium processor was a PGA chip that was placed in Socket 5 or Socket 7. Soon after its release, Intel marketed Pentium processors in 75, 90, 100, 120, 133, 150, 166, and 200 MHz flavors, which were really just clock multipliers of the original 60 MHz or 66 MHz systems.

*Clock multiplying* is the concept that the processor will run faster than the motherboard that the processor sits in. For example, the original Pentium processor ran on 60 or 66 MHz motherboards. Say that the computer is marketed as a Pentium 90. Because you know that the motherboard runs at 60 or 66 MHz, you can determine that the 90 comes from  $60 \times 1.5$  — meaning that the processor runs 1.5 times the speed of the motherboard. This is important because as a consumer, when you purchase a computer, you also want to make sure you know what the motherboard speed is — not just the advertised speed of the processor.

From a consumer's point of view, clock multipliers become important when you take a look at computers such as the Pentium 133 and the Pentium 150. Which is faster? The obvious answer is the Pentium 150, the system with the higher megahertz speed. But is it really? The Pentium 133 is a clock double of the 66 MHz board, and the Pentium 150 is a clock double and a half of the 60 MHz board. My point being that the overall performance of the system is controlled by more than just the speed of the processor — you need to consider other components, such as the speed of the motherboard.

By looking at the motherboard speeds of the Pentium 133 and the Pentium 150, you could assume that the computer running the Pentium 133 might be able to keep up with (if not outperform) the one running the Pentium 150. [Table 2-2](#) compares the speed of the motherboard and processor for the different Pentium systems. You do not need to memorize this table for the A+ exams; it is here to help you visualize clock multipliers as that is still being used in today's systems.

### **TABLE 2-2 Pentium Clock Multipliers**

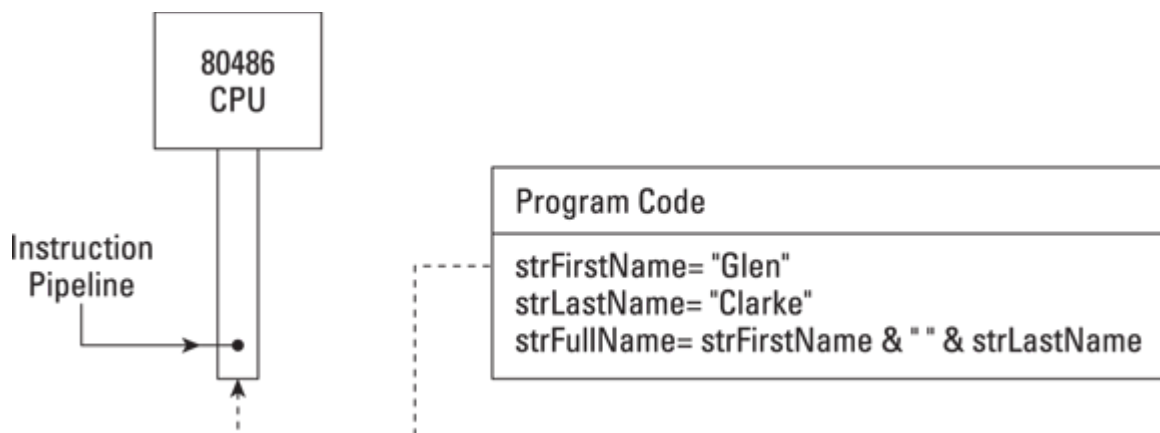
---

---

<b>Processor</b>	<b>Motherboard Speed (MHz)</b>	<b>Multiplier</b>	<b>Processor Speed (MHz)</b>
Pentium 90	60	1.5	90
Pentium 100	66	1.5	99
Pentium 120	60	2	120
Pentium 133	66	2	132
Pentium 150	60	2.5	150
Pentium 180	60	3	180
Pentium 200	66	3	198
Pentium II	100	4.5	450

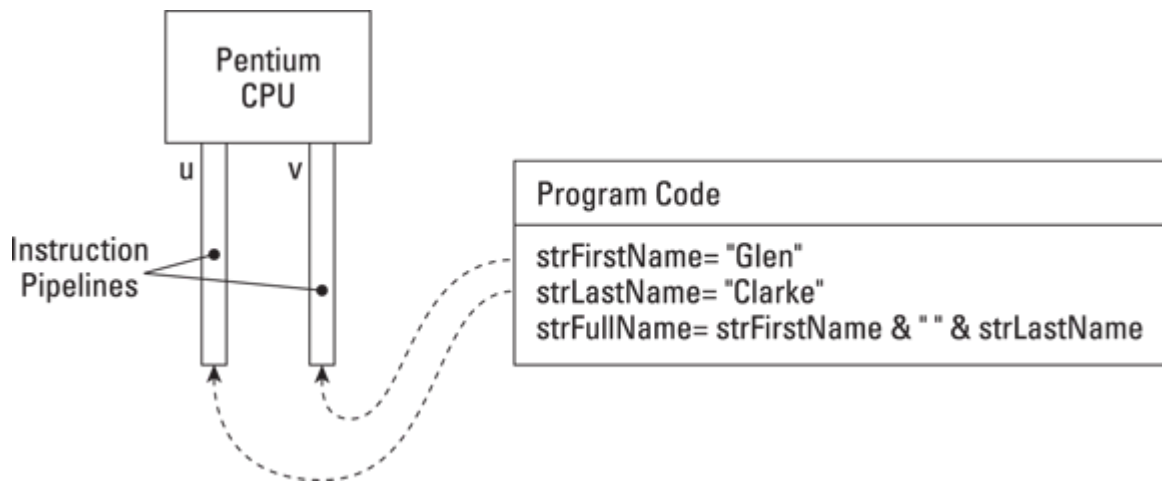
The Pentium processor has a 32-bit address bus, 32-bit registers, and a 64-bit data bus. It also has 16K of L1 cache that is divided into two 8K channels. One channel is for data cache and the other for application code cache.

Before the Pentium came along, processors used one *instruction pipeline*. This meant that when an application executed, it would run each stage of the application job one step after the other. For example, if an application has three lines of code, as seen in [Figure 2-9](#), each line of code can be processed only after the previous line of code is fully completed. This creates a delay, or wait time, which slows performance.



**FIGURE 2-9:** Single-instruction pipelined processor executing application code.

The Pentium processor introduced a feature called *superscalar design*. The processor has two instruction pipelines, named U and V. Having two instruction pipelines enables the processor to execute two instructions at the same time. Thus, the three lines of program code, shown in [Figure 2-10](#), can be quickly executed on a Pentium processor because lines 1 and 2 are processed at the same time, causing line 3 to be processed that much sooner. Notice that lines 1 and 2 execute parallel to one another; therefore, *parallel processing* is taking place.



**FIGURE 2-10:** Dual-instruction pipelined processor processing application code.

An application has to be designed to take advantage of two instruction pipelines. These applications are often labeled something like Pentium Aware or Pentium Ready.

## ***Pentium Pro***

In 1995, Intel released the Pentium Pro chip, which added a new level of performance to the Pentium processor. The Pentium Pro had all the characteristics of the Pentium processor — such as a 64-bit data bus and 32-bit registers — but it increased the address bus to 36 bits, which means that the Pentium Pro could access 64GB of RAM. The speed of the Pentium Pro ranges from 120 MHz to around 200 MHz.

The Pentium Pro included two additional features on its chip that helped it outperform the original Pentium. First, the Pentium Pro chip is really a two-chip team. One chip was the actual processor (with 16K of L1 cache, like the Pentium chip), but the other chip holds an extra 256K of cache

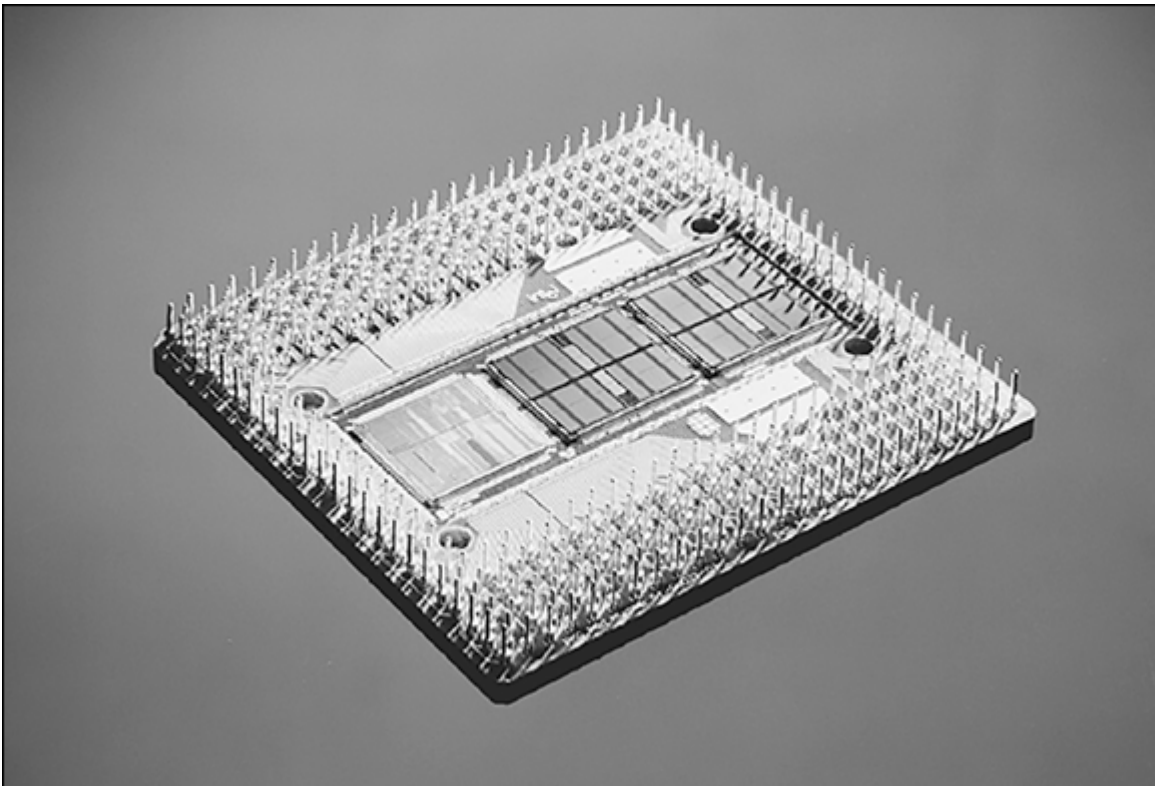


memory. Because this cache memory is physically outside of the CPU, it is considered L2 cache.

The second feature that led to the performance gain of the Pentium Pro is *dynamic execution*, which has three stages: multiple branch prediction, dataflow analysis, and speculative execution.

- » **Multiple branch prediction** is the idea that the processor will look ahead and predict a number of instructions that might be needed in the very near future.
- » **Dataflow analysis** occurs when the processor looks at the instructions it has predicted will be needed next and then assigns them a logical order of execution.
- » **Speculative execution** is the actual execution of a given instruction based on the prediction and the order of execution assigned.

The Pentium Pro chip, shown in [Figure 2-11](#), was implemented as a PGA chip that was placed in Socket 8.



**FIGURE 2-11:** The Intel Pentium Pro processor.

## *Pentium II*

In 1997, Intel produced the Pentium II, which was really just an enhanced Pentium Pro with speeds ranging from 233 MHz to 450 MHz. The Pentium II had a 64-bit data bus, a 36-bit address bus (64GB of RAM), and 32-bit registers; and supported features such as MMX.

The Pentium II increased the amount of L1 cache that was integrated into the CPU to 32K, as opposed to 16K. The 32K of L1 cache was still divided into two equal channels: one 16K channel for data and one 16K channel for application code.

Intel packaged the Pentium II in the *Single Edge Contact* (SEC) — sometimes also referred to as the *Single Edge Contact Connector* (SECC) — that fits into Slot 1 on the motherboard. The SEC is a module enclosed in a casing or shell with two chips inside: one chip being the processor, and the other chip being the 512K of L2 cache. Refer to [Figure 2-9](#) to see what a Pentium II processor, which uses the SEC, looks like.

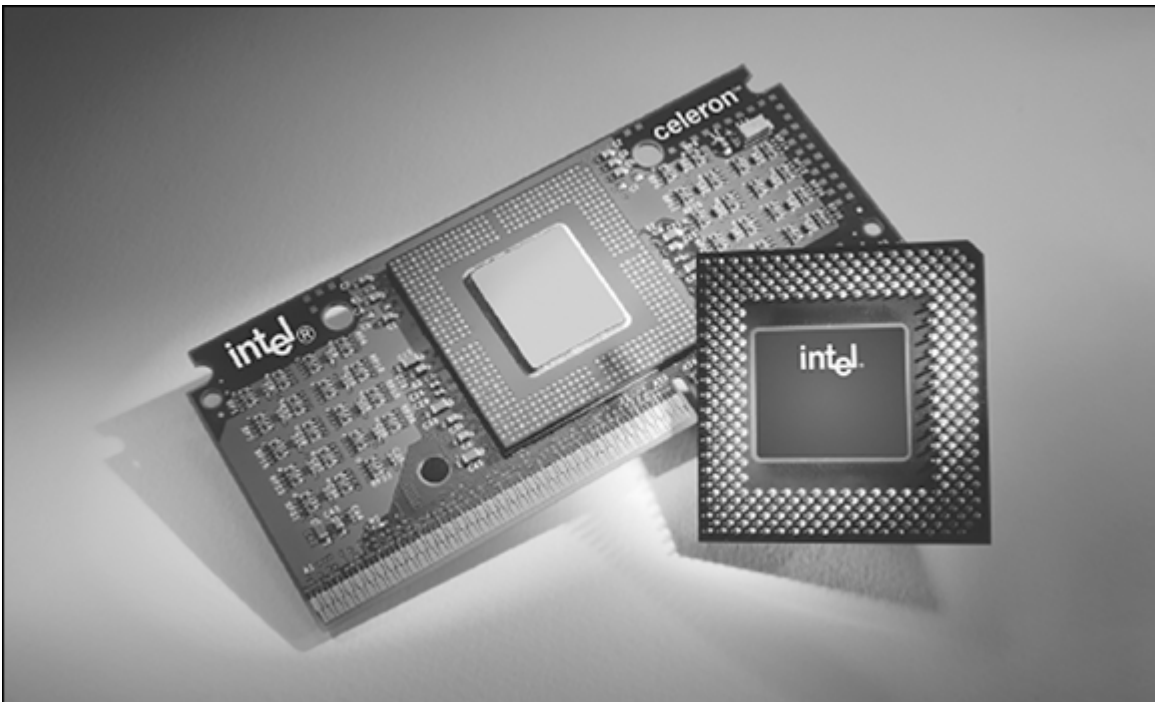
Another enhancement that accompanied the Pentium II was single instruction multiple data (SIMD). To visualize how SIMD works, imagine five toddlers in a playroom, and that these toddlers are at the entertaining age of two — the age, of course, when the toddlers are preparing for their teen years by answering “no” to everything you say. You walk into the playroom and see that the five toddlers have found your box of darts and are throwing them at the walls. You are faced with a choice: You can either walk around to each child and explain why throwing darts at your walls is not a good idea (which means you will have to explain the same thing five different times), or you can have a good scream at the top of your lungs, which means that all the children will stop immediately and listen. SIMD works on the same basic principle. With SIMD, the processor gives the instruction to multiple processes at once instead of having to give the same instruction multiple times. Thus, the processor saves time and creates a much more efficient way to work with information.

## *Celeron*

The Pentium II processor performed very well, and with all that cache memory, it should! Unfortunately, that performance came with a price. If you were not willing to pay that price, Intel created a chip for you: the Celeron chip!

The Celeron chip is nothing more than a less-expensive version of the Pentium II processor with the built-in L2 cache either removed entirely or reduced. The first-generation Celeron chip was code-named the Covington; it has no L2 cache memory on it. The second-generation Celeron was code-named the Mendocino, and it contains 128K of L2 cache. Although this version of the Celeron does have L2 cache, it is dramatically reduced from the Pentium II's 512K so that it can be sold at a lower price.

The original Celeron shipped in an SEC package but also had a version that was packaged as a PGA, as shown in [Figure 2-12](#).



**FIGURE 2-12:** Intel's Celeron processor was first implemented as an SEC package, but later had a PGA chip that was placed in Socket 370.

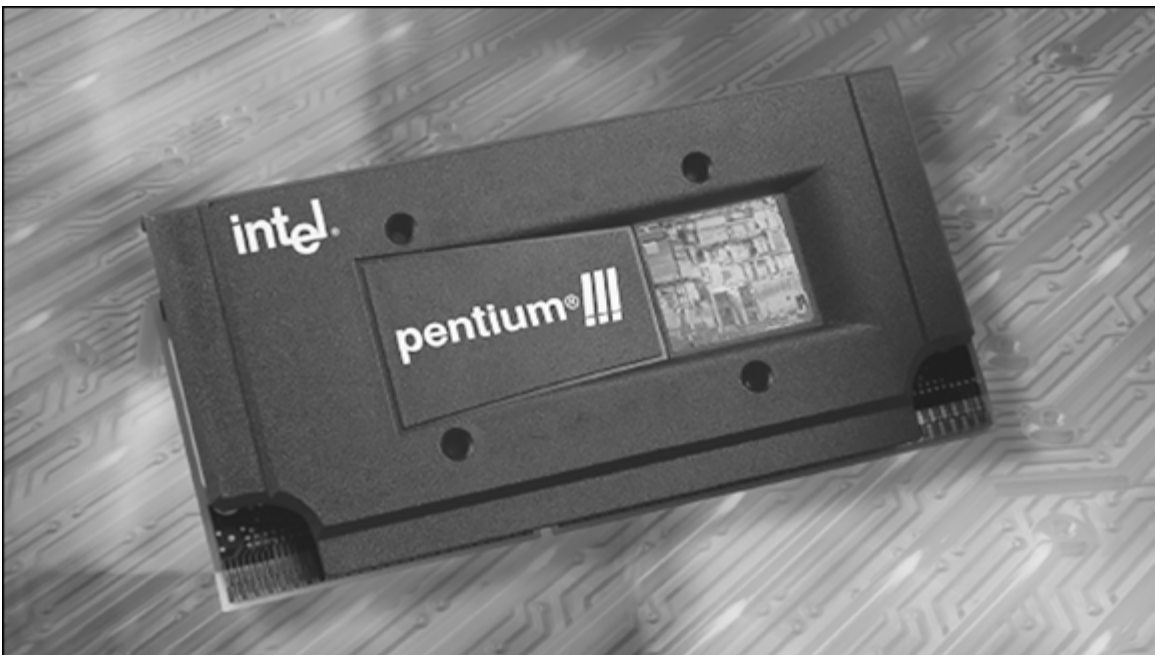
## *Pentium III*

The Pentium III processor shares many of the Pentium II characteristics. It supports dynamic execution (as the Pentium Pro also did) and MMX technology, has 32K of L1 cache, and has either 256K or 512K of L2 cache. The Pentium III runs at a speed of 450 MHz to 1000 MHz (1 GHz).

The Pentium III chip offers 70 additional instructions that are integrated into the chip, enhancing the user's experience with 3-D graphic applications. The Pentium III chip also supports a number of low-power states to help conserve energy when the system is not in use. This processor is designed to run on either 100 MHz or 133 MHz motherboards.

Also note that there is a Pentium III version of the Celeron chip that runs as fast as the Pentium III processor but again has the L2 cache memory reduced. So now there are multiple versions of the Celeron chip — the PII version and the PIII version.

The Pentium III processor shipped in the SEC2 package (as shown in [Figure 2-13](#)) originally, but was then packaged as a PGA chip. The SEC2 goes in Slot 1, and the PGA chip is inserted into Socket 370.



**FIGURE 2-13:** The Pentium III processor in the SEC2 package that lives in Slot 1.

## *Xeon*

The Xeon processor is built on the Pentium II and Pentium III architecture — meaning that, like the Celeron, there is a PII version and PIII version of the Xeon. The Xeon chip is designed for higher-end systems, such as server-class systems, and contains more cache memory than the typical PII and PIII. The Xeon comes in flavors of 512K, 1MB, and 2MB of L2 cache.

The Xeon can also address 64GB of RAM and is designed for *multiprocessing systems*: that is, computers with a motherboard that supports multiple CPUs. The Xeon processor has been designed to coexist with two, four, or eight CPUs.

The Pentium II Xeon and Pentium III Xeon chips were originally packaged as an SEC (as shown in [Figure 2-14](#)) that was placed in Slot 2, but later versions use the PGA and are placed in Socket 603. The Xeon chip also contains a thermal sensor that shuts the processor down if it starts to overheat.



**FIGURE 2-14:** The Pentium II Xeon processor was originally delivered in the SEC package.



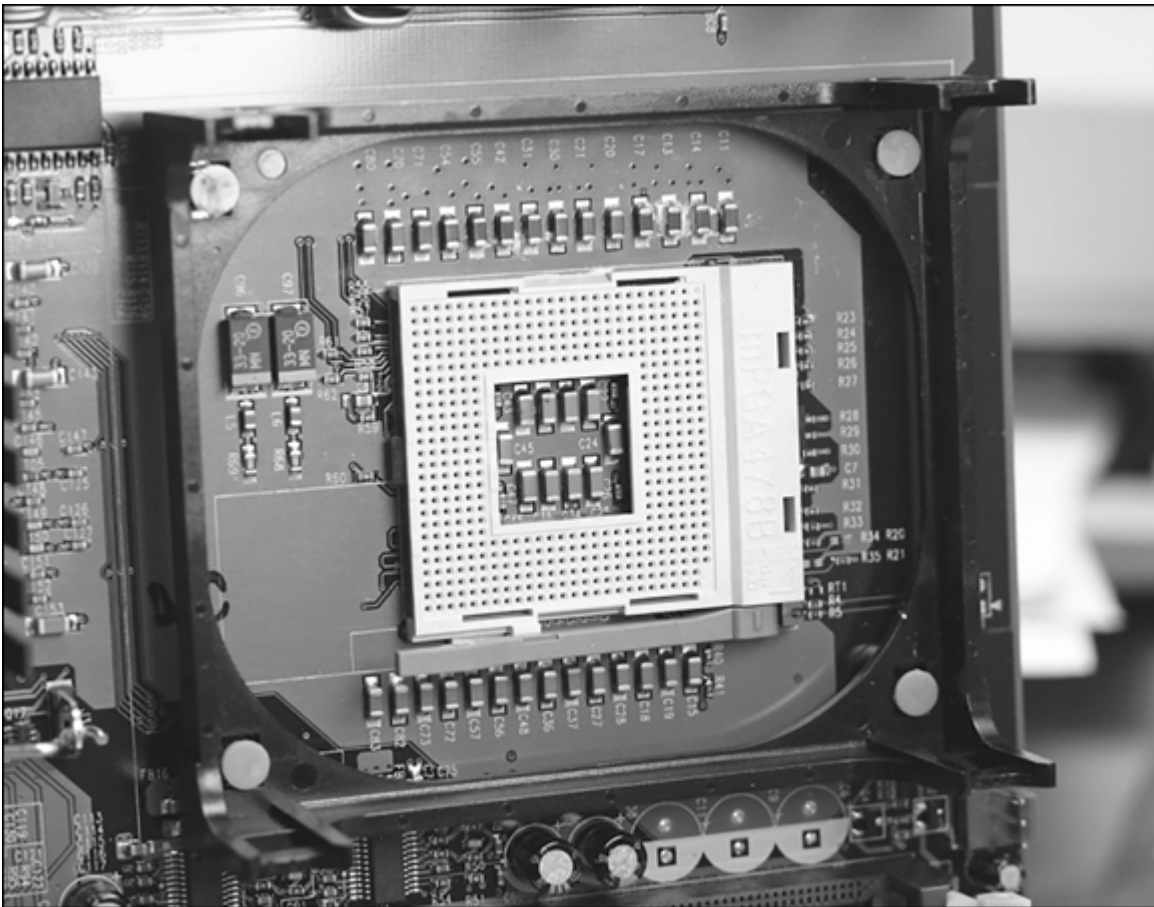
**REMEMBER** The Celeron is a scaled-down version of the Pentium II or III processor, and the Xeon is a step up from the Pentium II or III. There are also PIV (Pentium 4) versions of the processors:

- » **PIV Xeon:** Designed to work with a multiprocessing system that uses one or two processors
- » **PIV Xeon MP:** Designed to work with a multiprocessing system that uses four or eight processors

## ***Pentium 4***

The Pentium 4 processor runs between 2 GHz and 4 GHz. The Pentium processor has 20K of L1 cache and 512K of L2 cache. The processor is shipped as a 423-pin or 478-pin PGA package, which means that the chip will be placed in Socket 423 or Socket 478 (as shown in [Figure 2-15](#)).





**FIGURE 2-15:** Socket 478 can house a Pentium 4 processor.

The Pentium 4 processor gets a huge performance benefit by being able to perform four data transfers in one clock cycle along the *front side bus (FSB)*, which is the bus that connects the processor to system memory. (See [Chapter 1](#) of this minibook.)

Most Pentium 4 processors today are multicore processors and enjoy the performance benefits that multicore brings.

## *Itanium and Itanium II*

Intel created its first 64-bit processor in the Itanium and Itanium II processors and was marketed for server class—system or high-end PCs. Although the Itanium is a 64-bit processor and designed to run 64-bit software such as the 64-bit version of Windows, the Itanium can run some 32-bit code with the use of an emulator, but the code will run slower than if it were on a 32-bit processor. Special 64-bit editions of Windows can

run on the Itanium processor, which enables you to take advantage of the 64-bit architecture.

The original Itanium processor used a special packaging known as the *pin array cartridge (PAC)*, which uses 418 pins. The Itanium II was packaged in *organic land grid array (OLGA)* — a variation of the PGA — but the chip is located on a *processor card* (a circuit board that holds the processor). The OLGA fits into Socket 611.

The Itanium processor runs at around 1 GHz and contains a large block of cache memory: 32K of L1 cache, 96K of L2 cache, and 2MB or 4MB of L3 cache. The L3 cache is an additional block of cache memory located in the chip packaging.



**TIP** Moving from 32-bit processors and applications to 64-bit versions would truly benefit any user using applications that are memory intensive or calculation intensive. For example, a user who works a lot with multimedia-type applications would see an improvement in performance.

## *Pentium M*

For years, laptop manufacturers have been asking for smaller processors to place in laptop systems, and they finally have their wish. A number of processors have come out with the M version, which stands for *mobile*. The mobile versions of the processors are smaller than the processors that go in desktop systems, so they fit better and also use a lot less power. The benefit of using less power also means that they run much cooler.



**REMEMBER** Because the mobile versions of the processors use less power, they also run a little slower than their desktop counterparts.

Some popular brands of mobile processors are the Intel Pentium III M and the Pentium M. Intel's big competitor, AMD, also has mobile versions of its processors: Athlon XP M and Mobile Duron. (Some manufacturers put



the word *mobile* in the name of the processor instead of the letter *M*.) The next sections discuss more about AMD processors.

## ***Intel Core 2***

Intel designed the Intel Core 2 to be its 64-bit, multicore processor. The Core 2 comes in three flavors:

- » **Core 2 Solo:** Single-core processor
- » **Core 2 Duo:** Dual-core processor on the one chip
- » **Core 2 Quad:** Actually two chips, with two cores per chip, packaged in a multichip module

Core 2 processors range in speed from 1 GHz to around 3 GHz and fit into an LGA 775 socket, also known as Socket T. Core 2 processors come with either 2MB of L2 cache or 4MB of L2 cache.

## ***Intel Atom***

Intel has created a processor to run on the now-popular Netbooks. A Netbook is a laptop-like computer — but much smaller — that is used primarily for Internet usage. The Netbook is much smaller and cheaper than a regular laptop system and is marketed for email and web browsing features.

The Intel Atom has many characteristics of normal processors — it runs between 1 GHz and 2 GHz and contains 32K of L1 cache and 512K of L2 cache. Originally the Atom processor had one instruction pipeline, but there are versions with two instruction pipelines. There are also single core and dual core versions of the Atom processor.

## ***Intel Core i3/i5/i7 processors***

Intel has created a family of processors to satisfy lightweight system use or heavy system use that needs a powerful processor. The following are three common Intel processors found in new systems today:

- » **Intel Core i3:** The Intel Core i3 processor is the least powerful of the three processors and ships with an integrated GPU and two processor

cores. The i3 typically has a 64KB L1 cache, 256KB of L2 per core, and a shared block of L3 cache of approximately 3MB.

- » **Intel Core i5:** The Intel Core i5 is the next step up with similar specs but with more power. The i5 processor can contain between two and four processor cores, with L3 cache memory ranging from 3MB to 8MB.
- » **Intel Core i7:** Intel's highest-level processor is the Intel Core i7, which ships in different flavors as well. Depending on the model, the i7 ships with four or eight cores and an L3 cache ranging from 6MB to 12MB.

**Note:** The Intel Core i3, Intel Core i5, and Intel Core i7 processors are on their 6th generation now. When purchasing a system, be sure to know the generation of these processors. The newer generations have improvements to the architecture to make the system run faster. For example, the third generation Intel Core i7 uses *Intel Turbo Boost Technology 2.0*, which allows the processor to dynamically increase the processor speed when it needs it. Also note that the third generation of these processors integrates the graphics engine right into the processor chip to improve visual performance when gaming.

When upgrading a system, knowing the socket type can help you identify the generation of the Intel Core processor you are dealing with. Also knowing the generation of the processor can help you identify the socket type. For example, a Sandy Bridge Core i3 processor uses LGA 1155 but also does a Sandy Bridge Core i5 processor. This means if you have a motherboard with LGA 1155, you can upgrade the i3 to an i5 processor. Refer back to [Table 2-1](#) and have a look at the Intel Core i3/i5/i7 sockets. Also note that *Sandy Bridge* is the code name for the second generation of the Intel Core processors. Each generation has a code name.

## *Don't Forget Non-Intel Chips*

One of Intel's major competitors is Advanced Micro Devices (AMD). AMD has developed a family of processors that compete with Pentium-

class processors. In this section, I provide an overview of some of the characteristics of the AMD processors.

## ***K6***

The AMD K6 processor was designed to compete with the original Intel Pentium. The K6 has 64K of L1 cache, supports MMX technology, and has built-in branch prediction techniques. This processor has 321 pins, which means that it will fit into a Socket 7–supported motherboard.

## ***K6-2***

The K6-2 processor was designed to compete with the Pentium II chip. It has 64K of L1 cache and 256K of L2 cache. The K6-2 also supports dynamic execution, MMX technology, and superscalar design.

The K6-2 has added *3DNow!* technology, comprising a number of additional instructions integrated into the chip to improve 3-D graphics applications. The K6-2 chip also uses a 100 MHz motherboard speed, which is a big improvement over the 60/66 MHz motherboard speed that the original Pentiums used.

The K6-2 has 321 pins, which means that it will fit into a Socket 7–supported motherboard.

## ***K6-III***

The K6-III processor is designed to compete with the Pentium III chip. This chip shares many of the features of the K6-2, including a 100 MHz system bus. One of its features was the tri-level cache. Not only can it take advantage of an L1 and L2 cache but also an L3 cache that can be included on the motherboard.

## ***Athlon***

The AMD Athlon chip has 128K of L1 cache and 512K of L2 cache. It supports improved dynamic execution, MMX technology, and *3DNow!* technology. The Athlon chip runs at speeds of up to 1.2 GHz and is designed to run on a 200 MHz system bus speed.

Unlike the K6-2 and K6-III, the Athlon is not a PGA-packaged chip that supports Socket 7. It uses its own socket type — Slot A, so called

because the processor is packaged as an SEC. The Slot A socket is not compatible with Intel's Slot 1, which means that users have to purchase a motherboard designed for the Athlon chip.



**REMEMBER** Later versions of the Athlon moved to the PGA package that has 462 pins. These PGA chips are placed in Socket A.

## *Athlon XP*

After the Athlon chip was produced, Intel created the Pentium 4 chip. So AMD wanted to create a competing chip for the Pentium 4: namely, the Athlon XP. The Athlon XP is packaged as a PGA with 462 pins and is placed in Socket A. The Athlon XP runs at 2 GHz or more and contains 128K of L1 cache and 512K of L2 cache.



**TECHNICAL STUFF** AMD markets these processors a little differently. Instead of labeling the processor with its speed, AMD labels it with its competitor's speed. For example, the Athlon XP 1800+ is rated at 1.6 GHz but runs as fast as the Intel 1.8 GHz processor.

## *Duron*

AMD wanted to create a processor that competed with each version of the Intel processors. So, if the Athlon XP competes with the Pentium 4, what competes with the Celeron? You guessed it — the Duron.

The Duron has 128K of L1 cache and 64K of L2 cache. This processor is packaged as a PGA with 462 pins, which means that it, too, goes into Socket A.

## *Opteron*

Just like the Duron was built to compete with the Intel Celeron, AMD created the Opteron to compete with Intel 64-bit Itanium processors. The

Opteron runs at about 1.8 GHz and contains 128K of L1 cache and 1MB of L2 cache.

The Opteron is packaged with a micro-PGA, which is made up of 940 pins and is placed in Socket 940. One of the major differences between the Opteron and the Itanium is that the Itanium cannot run 32-bit applications. AMD decided that the Opteron would run in a 32-bit *or* 64-bit mode, thus allowing it to run 32-bit applications.

## ***Athlon 64 and Athlon 64 X2***

The Athlon 64 — the successor to the Athlon XP — is the AMD 64-bit processor for desktop systems. The Athlon 64, with 128K of L1 cache and at least 512K of L2 cache built into the processor, is designed to compete with the Pentium 4.

Although the Athlon 64 is a 64-bit processor, it has been designed to be backward compatible; it can run 32-bit code. The Athlon 64 X2 is the dual-core version of the Athlon 64. The Athlon 64 family processors fit into a number of sockets: Socket 754, Socket 940, and the AM2 socket.



**FOR THE  
EXAM**

Know that the Sempron processor is a low-end version of the Athlon 64 and has replaced the Duron as the AMD low-end processor. The Sempron was originally a 32-bit processor with reduced cache size, but current versions are 64-bit with the cache size reduced.

## ***Phenom and Phenom II***

The Phenom and Phenom II pick up after the Athlon 64 and are the AMD triple- and quad-core processors. The Phenom, designed for desktop systems, uses the code names Toliman for the triple-core version and Agena for the quad-core version.

The Phenom processor, which comes with 128K of L1 cache and 512KB of L2 cache per core, also has 2MB of shared L3 cache. The processor

fits in the AMD AM2+ socket and runs between approximately 1.8 GHz and 2.6 GHz.

The Phenom II also sits in the AM2+ socket and increases the shared L3 cache to 6MB! There were issues with the Phenom running on Windows Vista, but those bugs have been fixed for the Phenom II. The Phenom II has a triple-core version, code-named Heka, that runs between 2.6 GHz and 2.8 GHz. The quad-core version that is named Deneb runs between 2.5 GHz and 3.0 GHz.

### ***Turion 64 and Turion 64 X2***

The Turion 64 processor is the AMD 64-bit mobile processor for use in laptop computers. The Turion processor used to be called the Athlon Mobile 64, but AMD has moved to the new label of Turion 64 for its mobile processors. The Turion 64 is a single-core processor, and the Turion 64 X2 is the dual-core processor.

Turion 64 processors come with 128K of L1 cache and either 512K or 1024K of L2 cache. Both the Turion 64 and the Turion 64 X2 fit into Socket 754, and the newer chips fit in AMD Socket S7.



**FOR THE  
EXAM**

Be sure to know the multicore processors for the A+ exams. The Athlon 64 X2 is the AMD dual-core processor, and the Phenom/Phenom II have triple-core and quad-core versions. Also be familiar with the Turion being the AMD 64-bit processor for laptop computers.

## ***Installing a Processor***

Now that you understand some of the popular processors that exist today, take a look at how to install a processor. This section identifies installation decisions you have to be aware of before actually attempting to install the processor.

## *Will it fit in the socket?*

The first thing you need to verify before you purchase a new processor for your system is what socket type you have on your motherboard. You want to make sure that you purchase a processor that fits in that socket. For example, if you have Socket A on the motherboard, what processors fit in Socket A? If you said Athlon, Athlon XP, and Duron, you are correct.

Also be sure you know how many pins the socket has because some processors support a few differently sized sockets. For example, Intel makes both Socket 423 and Socket 478 versions of the Pentium 4, so make sure you get the correct version of the Pentium 4 for your socket.

## *CPU voltage and transistor integration*

Another important CPU characteristic that you have to watch for when upgrading your processor is the voltage the processor requires. *Voltage* is the power that the processor draws from the main motherboard, which the motherboard receives originally from the power supply.

A processor is designed to run at a certain voltage. You need to ensure that the motherboard you are placing the processor into provides that voltage. If a motherboard supports more than one voltage, you can typically change a jumper on the motherboard, which will then control the voltage used by the processor. For more information on jumpers, check out Book 2, [Chapter 1](#).

## *Performing the installation*

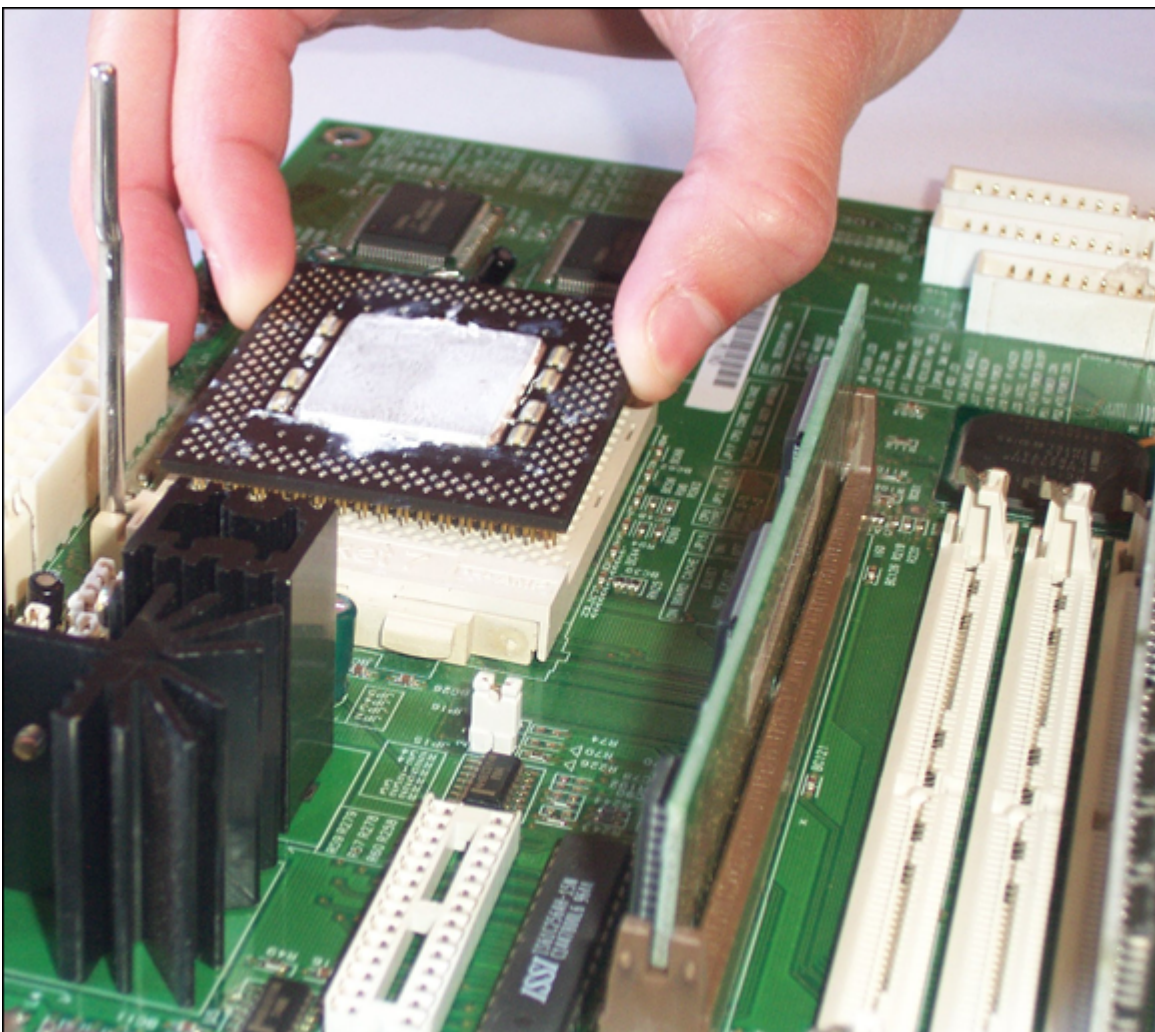
Because most systems today use ZIF sockets and PGA chips or LGA chips, I discuss installing a processor into the ZIF socket. After you verify that your new processor will work with your motherboard, you are ready to install the processor. To install the processor, first remove the existing one by pulling up on the lever on the ZIF socket. When you pull the lever on the ZIF socket, the existing processor should rise out of the socket a bit.





**WARNING** Be sure to ground yourself before touching the insides of a computer. Get an antistatic wrist strap and clamp it to the computer's chassis so that you have a constant ground. For more information on safety procedures, read Book 1, [Chapter 3](#).

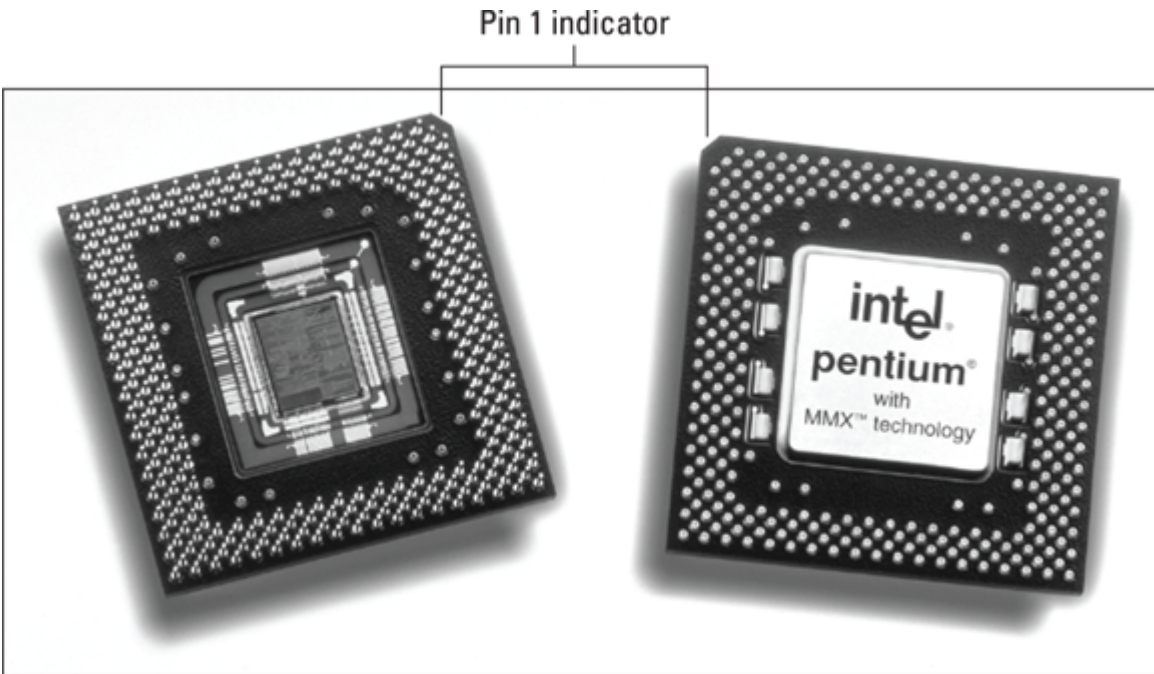
With the processor a bit out of the socket, you can then gently lift out the processor (as shown in [Figure 2-16](#)). Be sure to lift the processor straight up so that you do not bend any of the pins.



**FIGURE 2-16:** Removing the processor from its socket.

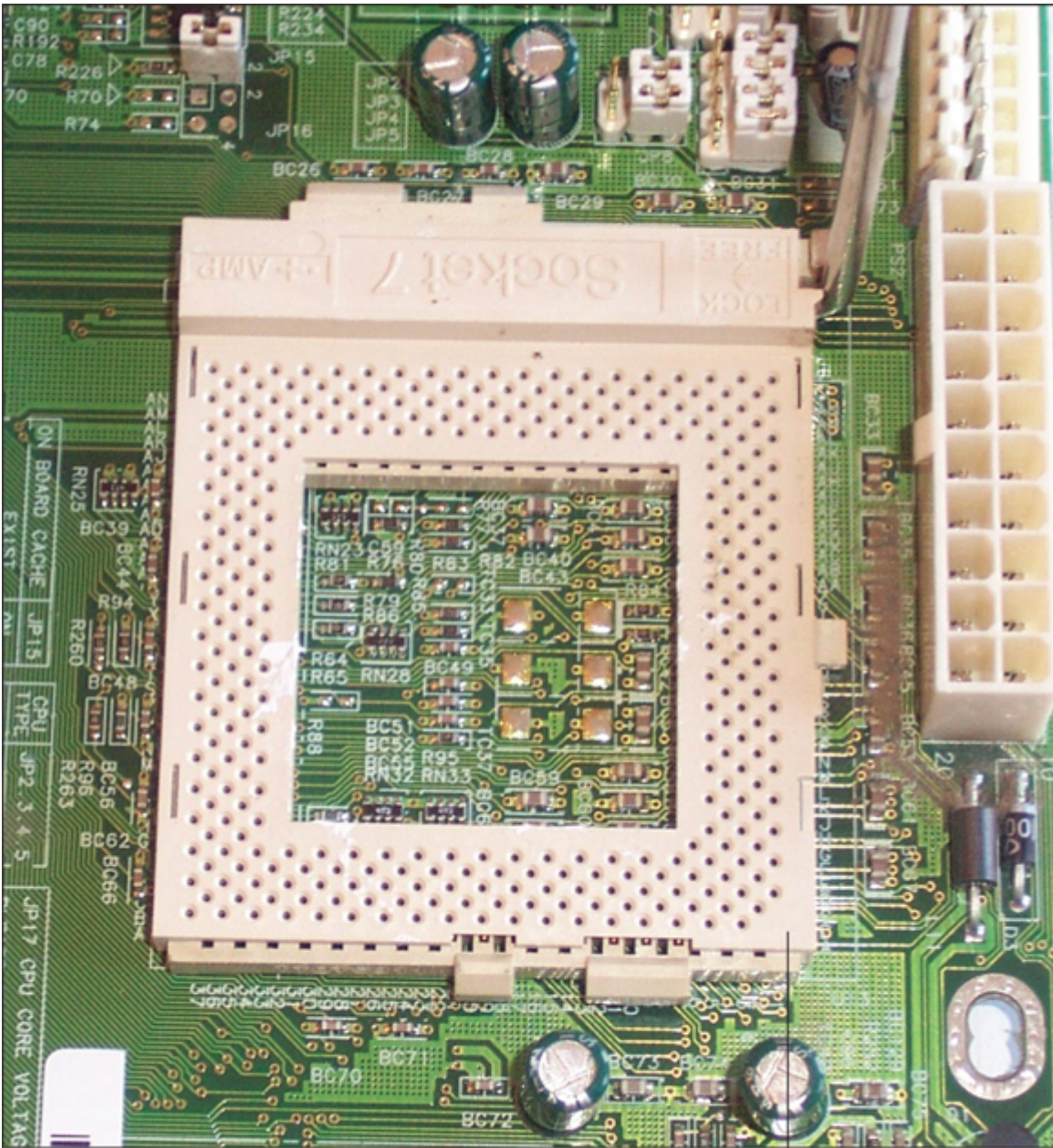


After you have the old processor out of the socket, you can install the new processor by first finding out where pin 1 is on the processor chip. Pin 1 is located in one of the corners of the chip and is usually indicated with a gold line marked on the bottom of the chip that contains the pins. If you do not see a line indicating where pin 1 is, you will notice that one of the corners of the square PGA is cut off (see [Figure 2-17](#)) — this corner is pin 1.



**FIGURE 2-17:** The cut-out corner of the processor indicates the location of pin 1.

After you locate pin 1 on the PGA chip, you also need to figure out where pin 1 goes in the socket. Again, you can figure this out by finding the cut-off corner of the socket. This corner is where the cut-off corner of the processor goes, as seen in [Figure 2-18](#).



Pin 1 indicator

**FIGURE 2-18:** Identifying the cut-out corner in the processor socket.

After you match up pin 1 on the PGA chip with pin 1 on the ZIF socket, carefully place the processor into the socket and then push the lever down to lock it in place.



**WARNING** Just lay the chip into the socket; don't push it in. The whole point of a *zero insertion force* socket is that you don't have to risk damaging the pins by applying pressure.

Note that newer processors, such as LGA, will have the socket and processor keyed so that you cannot put the processor in the wrong way. For example, my Intel Core i5 processor has little notches on the side that allow it to only fit in the processor socket one way.

## *Keeping a Processor Cool*

After you have the processor in the processor socket, you need to install something to keep it cool, such as a heat sink or fan — or maybe even both.

Processors are made up of thousands, even millions, of transistors. A *transistor* acts as a switch, permitting or prohibiting the flow of electrical current. If current is allowed to flow through the transistor, some result is generated. If the current is not allowed to flow through the transistor, a different result is generated.

A processor contains millions of transistors that each hold an electrical charge, causing the processor to run at very high temperatures. Therefore, it is important to keep the processor cool. The most common cooling mechanisms today are heat sinks and CPU fans, which are sometimes used in tandem.

A number of other cooling devices are on the market today, and they are a little more expensive than your typical heat sink or CPU fan. The following are other cooling techniques you may find in systems today:

- » **Liquid-based cooling:** A liquid cooling system pumps a cooling liquid throughout the PC by using small hoses. The benefit of a liquid cooling system is the reduced noise, but its big drawback is the amount of space needed in the PC for the components of the cooling

system — and, of course, the threat of a leak if the cooling system is not installed properly.

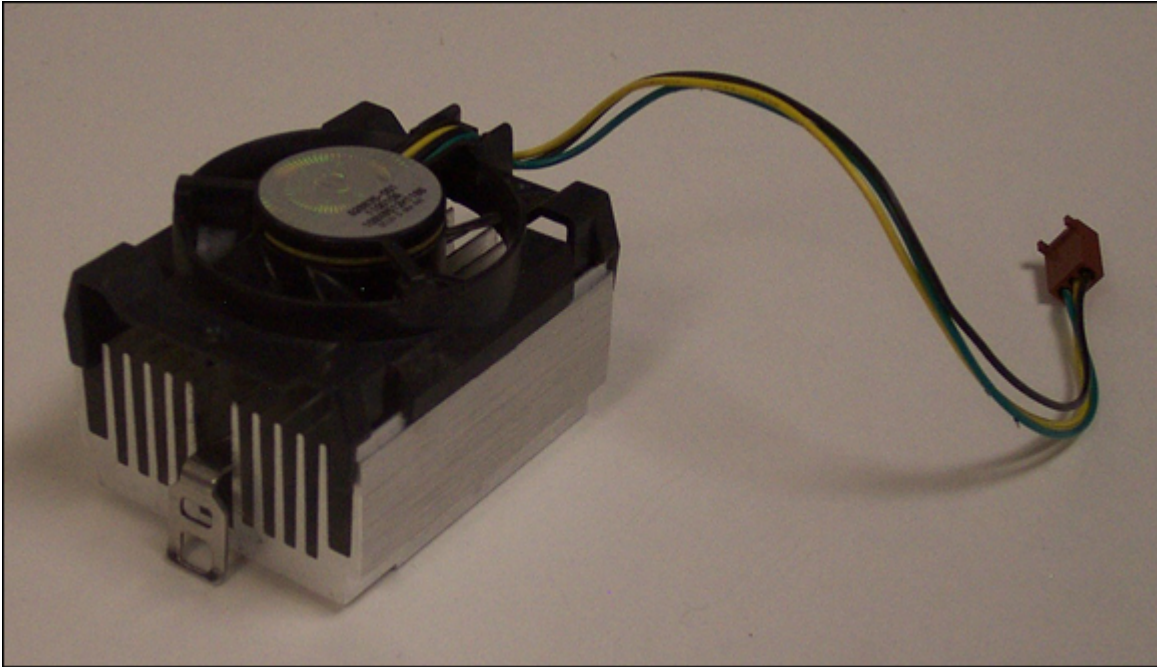
- » **Temperature sensors:** A number of processors today come with a built-in thermal sensor (a high-tech thermometer). Temperature sensors allow the processor to identify that it is overheating and then shut itself down until the temperature drops to normal.
- » **Thermal paste:** This paste is placed between the processor and the heat sink to help draw the heat away from the processor and pass it through the heat sink.
- » **Fanless/passive:** There are also fanless, or passive cooling mechanisms that can be used to cool processors. These essentially look like a spinning heat sink, but they do not have a noisy fan sitting on top to keep it cool. There are two major benefits of this cooling technique over fans: They are quiet and they do not collect dust.
- » **Heat pipes:** A heat pipe is designed to transfer heat from a hot temperature source by vaporizing a form of coolant liquid that is then vacuumed away from the heat source to a cooler interface. The vapor can then be rerouted from the cool source to the heat source again as a liquid to perform the cooling process again.

## *Heat sinks and CPU fans*

Because of the size of the Pentium processor and the number of transistors passing current, the chip can get so hot that it becomes unstable. Thus, many Pentium processors come with either a cooling fan or heat sinks. A number of processors today have a heat sink with a fan on top of the heat sink.

*Heat sinks* are a group of metal pins placed on the chip to draw heat away from it. A *cooling fan* is a small fan placed on top of the processor to pull away hot air, helping to keep the processor cool. [Figure 2-19](#) shows a heat sink.

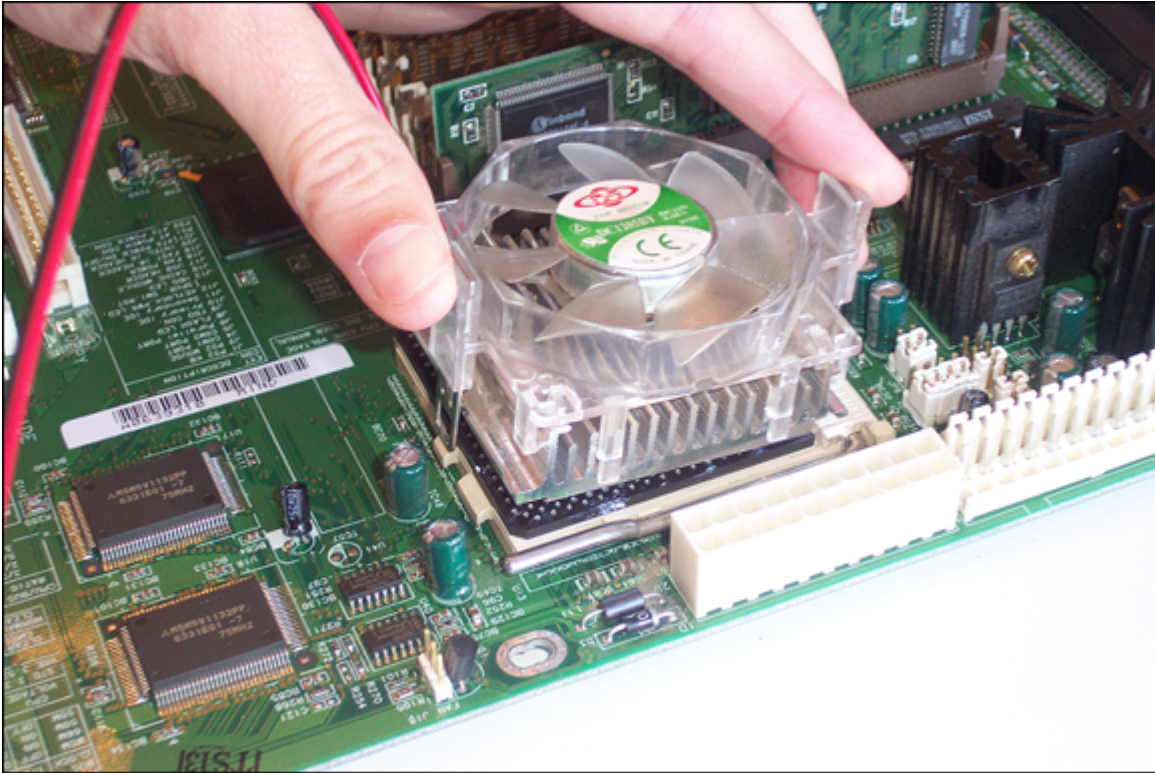




**FIGURE 2-19:** Looking at a heat sink.

### *Installing a heat sink and fan*

Some processors can get so hot that a heat sink might not be enough of a cooling device; in this case, you might want to place a fan on top of the heat sink. To install the heat sink and fan on your system, simply place the heat sink on the processor and then clamp it in place with the heat sink-clamping bar. After you have the heat sink in place, you can secure a fan on top of it by clamping the fan on the heat sink, as shown in [Figure 2-20](#).



**FIGURE 2-20:** Placing the fan on top of the heat sink.



**FOR THE  
EXAM**

The term *passive heat sink* is used for a heat sink that does not use a fan on top, and the term *active heat sink* is used for a heat sink with a fan on top.

## *Increasing Performance*

When it comes to processors, there are a number of different ways to increase the performance of your system. A first and obvious way is to buy the faster processor when upgrading; for example, upgrade a 1.8 GHz processor to a 3 GHz processor if possible. Also, get a processor designed to run on the faster motherboards. Many people just look at the speed of the processor and not the speed of the motherboard that the processor is sitting in. You can increase overall performance of your system by purchasing the faster motherboard.

You will have to look at other features of the processor, such as the L1 cache and L2 cache that reside in the processor packaging. Acquiring a processor with more cache memory can dramatically increase system performance.

## *Getting an A+*

This chapter provides an overview of the key terms that are used to identify the popular processors and their capabilities. Some of the points you need to remember when preparing for the A+ exams are

- » **Chip packages:** The four major chip packages are DIP, PGA, SEC, and LGA. PGA was the popular chip packaging used for many years, but newer processors are using LGA.
- » **Processor speed:** Processor speed is measured in gigahertz (GHz) but was measured in megahertz (MHz) in the past.
- » **Cache memory:** In older systems, L1 cache was cache memory integrated into the processor chip, while L2 cache was found on the motherboard. With today's systems, each processor core has a block of L1 and L2 cache, while the processor has a block of L3 cache that is to be shared by all cores in the processor.
- » **Sockets:** A socket is used to hold the processor in place on the motherboard. Be sure to be familiar with the sockets for the Intel Pentium III, Pentium 4, and Celeron chips. Also know about the sockets for the AMD Athlon, Athlon XP, and Duron chips.
- » **Chips:** Be sure to review the characteristics of different Intel chips and AMD chips.

## *Prep Test*

**1. Which of the following best describes superscalar design?**

- (A) The processor is designed using only 3.1 transistors.

- (B) The processor predicts the next few instructions to be executed and then determines the optimal order for the execution of these instructions.
- (C) The processor has two instruction pipelines, which enables multiple instructions to execute at the same time.
- (D) The processor works twice as fast as the motherboard.

**2. You are upgrading the processor on one of the workstations for your customer. You remove a second generation Intel Core i3 processor. Which of the following can you upgrade to?**

- (A) Intel Core i5 (Lynnfield)
- (B) Athlon X4
- (C) AMD Opteron
- (D) Intel Core i5 (Sandy Bridge)

**3. You are upgrading an older system for your customer and notice that the system has Socket A on the motherboard. Which of the following CPUs are placed in Socket A? (Select all that apply.)**

- (A) Pentium III
- (B) Athlon XP
- (C) Celeron
- (D) Pentium 4
- (E) Duron
- (F) Itanium

**4. What chip type was the original Pentium processor packaged in?**

- (A) SEC
- (B) PGA
- (C) DIP
- (D) LGA



- 5. You have a processor that contains four cores. Which of the following best describes the L3 cache with this processor?**
- (A) There is a block of L3 cache shared by all cores.
  - (B) Each core has its own block of L3 cache.
  - (C) The odd number cores share a block of L3 cache, while the even number cores share a different block of L3 cache.
  - (D) The first core has exclusive use of the L3 cache.
- 6. Which of the following acts as a storage container for information that will be processed by the processor?**
- (A) Data bus
  - (B) Address bus
  - (C) Registers
  - (D) Math co-processor
- 7. You have a new system running an Intel Core i5 processor. You are studying for the A+ exams and need a few virtual machines to test the configuration of different operating systems. You install Hyper-V to create some virtual machines but then receive an error when you go to start a virtual machine. What could be the problem?**
- (A) EDB needs to be disabled in the BIOS.
  - (B) Create the virtual machines on a different drive than the operating system.
  - (C) Disable the integrated network card.
  - (D) Virtualization support needs to be enabled in the BIOS.
- 8. Which statement best describes the purpose of a math co-processor?**
- (A) Performs all logic functions on behalf of the processor
  - (B) Performs floating-point calculations on behalf of the processor
  - (C) Runs all applications, and a processor runs the operating system in a multitasking environment

(D) Allows for communication between devices

**9. You are upgrading the processor on a system and notice that the socket is a Socket R. What socket type is this also known as?**

(A) Socket 1155

(B) Socket 1150

(C) Socket 1156

(D) LGA 2011

**10. You have replaced the processor in an old system, and you are now ready to finalize the upgrade. Which of the following is the first item to use to help draw heat away from the processor?**

(A) Heat sink

(B) Thermal paste

(C) Fan

(D) Liquid cooling

**11. You are looking to add a Pentium 4 processor to one of the systems in your office. What sockets do Pentium 4 processors fit into? (Choose two.)**

(A) Socket 370

(B) Socket 423

(C) Socket 478

(D) Socket 920

**12. What is the major difference between a Celeron processor and a Pentium 4 processor?**

(A) The Celeron has more L1 cache memory.

(B) The Celeron has less L1 cache memory.

(C) The Celeron has more L2 cache memory.

(D) The Celeron has less L2 cache memory.

**13. Which of the following CPU characteristics determines how much total memory the system can access?**

- (A) Data bus
- (B) Address bus
- (C) Registers
- (D) Math co-processor

**14. What chip packaging type does an Intel Core i3 use?**

- (A) LGA
- (B) PGA
- (C) DIP
- (D) SEC

**15. Which processor is the AMD 64-bit processor designed for laptop systems?**

- (A) Core 2
- (B) Athlon 64
- (C) Phenom II
- (D) Turion 64

## *Answers*

1. **C.** Superscalar design is the idea that the processor has more than one instruction pipeline to process application code. Choice B describes a feature called *dynamic execution*, and choice D describes a clock double chip. See "[\*Pentium\*](#)."
2. **D.** The second-generation Intel core processors has the code name Sandy Bridge and is placed in LGA 1155. Therefore, a second generation Core i3 processor (LGA 1155) can be upgraded to a Core i5 Sandy Bridge processor because it uses LGA 1155 as well. Review "[\*Intel Core i3/i5/i7 processors\*](#)."

3. **B, E.** AMD Athlon, Athlon XP, and the Duron chip are placed in Socket A. *Check out “[Don’t Forget Non-Intel Chips](#).”*
4. **B.** The original Pentium processor was packaged in the pin grid array (PGA) chip type, which fits into either Socket 5 or Socket 7. Socket 5 and Socket 7 are incorrect choices because they are not chip types; they are the names of sockets. Dual inline package (DIP) is an older type of packaging for processor chips, and SEC is the chip packaging used with Pentium II processors. *Peruse “[Pentium](#).”*
5. **A.** L3 cache memory is shared by all cores within the processor. Each core also has some L1 and L2 cache that is for itself. *Peek at “[Cache memory](#).”*
6. **C.** Registers are storage areas for information to be processed by the processor. The data bus is the pathway to system memory, the address bus controls how much memory can be recognized by the processor, and the math co-processor performs many of the complicated mathematical operations. *Look over “[Registers](#).”*
7. **D.** To take advantage of virtualization capabilities of the processor, you need to ensure that virtualization support is enabled in the system BIOS. *Study “[Virtualization support](#).”*
8. **B.** The math co-processor performs many of the complicated math operations on behalf of the CPU, and the CPU itself performs the logic functions. *Refer to “[Math co-processor](#).”*
9. **D.** Socket R is also known as LGA 2011, and is used to hold the Intel Core i7 for high-end desktops or servers. *Examine “[Identifying Socket Types](#).”*
10. **B.** Thermal paste should always be placed on the processor before adding the heat sink, and before placing the fan on top of the heat sink. *See “[Keeping a Processor Cool](#).”*
11. **B, C.** Pentium 4 processors have either 423 or 478 pins, so they are placed in either Socket 423 or Socket 478. *Review “[Pentium 4](#).”*
12. **D.** The Celeron chip is a cut-price Pentium chip. The L2 cache is decreased to save on cost. Celeron chips either have no L2 cache or

128K cache, and Pentium II, Pentium III, and Pentium 4 chips have 512K of L2 cache. *Check out “[Celeron](#).”*

13. **B.** The address bus dictates how much memory the CPU can address. The data bus is the pathway to system memory, and registers are storage areas for data being processed. *Peruse “[Address bus](#).”*
14. **A.** The Intel Core i3 uses an LGA chip packaging and is placed in LGA sockets. *Take a look at “[Chip packaging](#).”*
15. **D.** The Turion 64 is the AMD 64-bit mobile processor to be used on laptop systems. *Peek at “[Turion 64 and Turion 64 X2](#).”*

## Chapter 3

# What to Remember about Memory

---

### IN THIS CHAPTER

- » Understanding memory terminology
  - » Identifying RAM types
  - » Understanding DRAM types
  - » Working with memory modules
  - » Identifying parity and nonparity memory
- 

Finding out how much memory a computer has is one popular way to measure that computer's power and capabilities. Think about it: If someone asked you what kind of computer you have, what would you answer? Probably something like, "I have an Intel i7 Processor with 16 gigs of RAM." But why do we measure the power of a computer based on the amount of memory it has?

In this chapter, you discover the purpose of memory and some of the different types of memory found in computers today. This chapter also discusses issues that affect installing memory in personal computers and laptops.

## *Understanding the Types of Memory*

This section outlines different types of computer memory — anything that stores information either permanently or temporarily. Computers have two different flavors of memory: ROM and RAM.



FOR THE  
EXAM

Make sure you fully understand the different types of memory and their uses. You are sure to see a few questions on memory.

## *Remembering the purpose of memory*

Before you look at the different types of memory, you need to understand the purpose of memory. Think about your desk at home or in the office. Whether sitting at your home or office desk (working on a proposal or preparing for your A+ exams), chances are good that your desk is covered with documents, books, and papers. This desk is your work area, and its size dictates how many documents you can work on at any given time.

System memory works the same way. You have documents and applications stored on the hard drive. When you want to work on these documents, you open them and place them in the computer's work area. The work area (or desk space) for a computer is *system memory*. When you want to work with any application or document, the computer must retrieve that information from the hard drive and execute it from memory.

Assume, for instance, that your computer has 4GB of memory. You start up your system, which is running Windows 8.1, and decide to run Microsoft Word and Adobe Photoshop at the same time. Assume that you open two very large files in each application. Assume further that you are using 3GB of precious memory at this point — for the operating system (OS) to load, and memory for each running application. As you can see, your memory usage adds up quickly.

In this scenario, you are already using 3GB of memory, which leaves a scant 1GB of memory remaining. Assume that you are about to open a Photoshop document and copy and paste information from one file to another. To put it simply, you are running out of desk space. You can solve the problem in one of two ways:

- » **Do less work.** In other words, work in one application at a time. This is not an optimal solution, especially for business users who often need to run multiple applications simultaneously.

» **Get a bigger desk.** In computer terminology, install more RAM. When you install more RAM, you have a bigger desk to work on.

Now that you understand the general purpose of memory, it's time to dive into the different types of memory. For the A+ exams, you are required to know many different types of memory, which I outline in the following sections.

## ***Read-only memory (ROM)***

ROM is a type of memory that you cannot write to: hence its name, read-only memory. Information is written to ROM chips by the manufacturer, and this information cannot be changed. In the past, if ROM information needed to be updated, you had to remove the original ROM chip and replace it with an updated ROM chip from the manufacturer. Today, you can update the ROM by running a special software program downloaded from the manufacturer's website. In essence, you do not really have a ROM chip but rather have an EEPROM (more on EEPROM in a bit).



TECHNICAL  
STUFF

Software written to a ROM chip is *firmware*.

One of the major uses for ROM is storing the system BIOS (basic input-output system), which contains the Power-on Self-Test (POST) routines and other routines that initiate loading the OS. The BIOS also contains the low-level code that allows the system to communicate with hardware devices.



FOR THE  
EXAM

You need to know that the POST is part of the BIOS code stored in ROM. The POST contains routines that initiate OS loading as well as routines that make communication between hardware devices possible.

## ***EPROM***



*EPROM* (erasable programmable ROM) is a type of memory that normally cannot be written to because it is a variation of ROM. An EPROM chip is a special ROM chip that the manufacturer can reprogram by using a special programming device that uses ultraviolet light.

## ***EEPROM***

A newer implementation of ROM is electrically erasable programmable ROM (EEPROM), or flash ROM. The manufacturer writes the software instructions into the ROM chip, but you can update these instructions by running a special software setup program provided by the manufacturer. The software setup program is usually available through the manufacturer's website.



**FOR THE  
EXAM**

EEPROM (better known as flash ROM) is a ROM chip that can be rewritten with special EEPROM update software provided by the manufacturer of the chip.

Using EEPROM has become the typical way to update your BIOS. BIOS code is designed to work with certain hardware. As hardware improves, you need to update your BIOS code so that your system is aware of these hardware improvements. Therefore, the manufacturer places BIOS updates on its website to download for computer users running its particular BIOS. You just have to download the BIOS update program and then run the BIOS update on your system. The update rewrites the BIOS instructions, making the computer “more aware” of today's hardware.

Some examples where you will need to download a BIOS update from a manufacturer's website is if you want to update the capabilities (the BIOS) of your computer or your home router. In these scenarios, you navigate to the manufacturer's website and download the firmware (BIOS) update and then run it on your computer or supply the update into the administration pages of the home router.

## ***Random access memory (RAM)***

Of the two flavors of memory (ROM and RAM), RAM is probably the more fundamental. As I mention earlier, ROM is permanent memory, or permanent storage of information. As the computer's primary working memory, though, RAM stores information temporarily. RAM is *volatile*, meaning that it needs constant electrical current to maintain the information that resides in its chips. If the electrical current is lost, RAM contents are erased. Likewise, when a computer is powered off, all RAM contents are flushed out. The following sections discuss the different types of RAM.



FOR THE  
EXAM

You can expect a few questions about the different types of memory. Be sure that you are familiar with these different types of RAM.

## **DRAM**

*Dynamic RAM* (DRAM) is probably the most popular type of memory today and the one that you are most often going to upgrade. When someone says to you, "I have 1024 megs of dynamic RAM," he or she is talking about DRAM.

Dynamic RAM gets its name from the fact that the information stored in DRAM needs to be constantly refreshed. Refreshing involves reading the bits of data stored in DRAM and then rewriting the same information back.



TECHNICAL  
STUFF

DRAM is *single-ported*: You can read and write to the memory but not at the same time.

Older implementations of RAM measured the memory's performance based on how long it took the CPU to access that data. This time is measured in nanoseconds (ns; 1 ns equals one-billionth of a second). If you have memory that is 50 ns and your best friend has memory that is 70

ns, your memory is presumably faster. Your CPU receives the information from memory after waiting only 50-billionths of a second, whereas your best friend's CPU waits 70-billionths of a second.



**REMEMBER** The lower the number of nanoseconds, the better the performance.

The speed of older DRAM ranges from 60 ns to 80 ns. Today's implementations of DRAM measure the speed of memory in megahertz (MHz), typically matching the motherboard speed. For example, my Intel i7 computer has memory that is running at 800 MHz.

For more information on the types of DRAM, see the section “[Identifying the Types of DRAM](#),” later in this chapter.

## **SRAM**

*Static RAM* (SRAM) — so-called because the information held in its memory cells doesn't need to be refreshed — requires less overhead than DRAM to maintain the information stored in memory.

With speeds running from 10 ns to 20 ns, SRAM is much faster than DRAM. Because SRAM is faster memory than DRAM, it is also more expensive, which is why people add DRAM to their systems more often than they add SRAM.

SRAM is typically used for *cache memory*, which stores frequently used data and program code after it is read from slower DRAM. Think of cache memory as a bucket that sits beside the CPU and stores frequently used information. After the system has searched through DRAM once for specific information, it can store that information in the bucket for easy access later. The next time the data is requested, it is read from cache instead of from system memory.

Because cache memory is much faster than DRAM, the CPU first tries to retrieve the information from cache: specifically, L1 cache first and then L2 cache. If the information is not located in cache, the system then tries to retrieve the information from memory. If the information is not located in system memory, it then is retrieved from disk. Attempting to retrieve the

requested information from cache first reduces wait time if the information actually resides there because of how fast cache is compared with DRAM.



**REMEMBER** Cache memory (SRAM) stores frequently used data and program code. Because cache memory is faster than DRAM, retrieving information from cache means that the processor does not have to wait for the slower DRAM, thus enhancing system performance.

## ***CMOS RAM***

The *complementary metal-oxide semiconductor (CMOS)* is the area where the computer stores its configuration information, such as whether the computer has a floppy drive, the amount of memory installed, the date and time for the system, and the number and size of the hard drives that are installed. Think of CMOS information as an inventory list for the majority of components that are installed on the computer. For more information on CMOS, see Book 2, [Chapter 4](#).

Where is CMOS information stored? Is CMOS information stored on the BIOS chip, or perhaps another ROM chip? The answer is neither. In fact, if the information were stored on a ROM chip, you wouldn't be able to go into the CMOS setup program and change the configuration. Instead, CMOS configuration information is stored in a type of RAM called *CMOS RAM*.

CMOS RAM is a special, volatile RAM chip that stores the CMOS information. If power is lost, the information is wiped out. This could present a problem with regard to CMOS configuration because if CMOS RAM is wiped out, the computer forgets its inventory information and has to relearn it. To prevent this problem, computers have a small battery on their motherboards that maintains enough of a charge to prevent CMOS RAM from losing its data.



FOR THE  
EXAM

CMOS information is stored in CMOS RAM, which is volatile memory that maintains its information by using a battery stored on the system board.

## ***VRAM***

*Video RAM* (VRAM) is most commonly used on video accelerator cards to store values of pixels onscreen for refresh purposes. VRAM is the favored memory for video because it outperforms the other memory types because it is dual-ported memory: That is, it can be read from and written to at the same time. Comparatively, DRAM is *single-ported*, which means that the memory can be written to and read from, but not simultaneously — only one direction at a time. VRAM, however, allows you to do both simultaneously.

Video graphics cards today help relieve stress from the CPU because they have their own processor, a *graphics processing unit* (GPU) to handle the mathematical calculations related to graphics operations. These graphics cards also contain a large block of memory as well. Many graphics cards will contain video memory in the gigabytes with 2GB of VRAM not being enough to handle high-end games at high resolutions. Many gaming systems will require a video card with at least 4GB of VRAM to handle the high resolution of high-end games.

## ***Identifying the Types of DRAM***

DRAM is the most popular type of memory used in systems today. It is also the most popular type of memory that computer users add to their computers when upgrading memory. Therefore, you must understand the different types of DRAM and what types of DRAM outperform others.

Memory is organized into rows and columns, like a spreadsheet. Information is stored in the different cells, or blocks, that are created by the intersection of these rows and columns. With DRAM, the CPU requests data from the memory controller by sending the address of the

row and the address of the column for every block of data that needs to be read. The memory controller then fetches the information from that memory location. [Figure 3-1](#) shows two memory cells that hold data that the CPU wants to have.

	0	1	2	3	4	5
0						
1						
2						
3						
4						

**FIGURE 3-1:** Looking at how data is accessed in memory.

## *Synchronous DRAM*

*Synchronous DRAM* (SDRAM) is memory synchronized to the system board speed. This synchronized speed means that the data stored in memory is refreshed at the system speed, and data is accessed in memory at the system speed as well.

SDRAM is one of the most popular types of DRAM found in earlier Pentium systems, such as the Pentium II. When you upgrade memory on your system and you determine that you need SDRAM, you then need to determine what speed of SDRAM. Because you are running at the system speed, you must match the DRAM speed with the motherboard speed. Thus, if you have a 100 MHz motherboard, you need 100 MHz SDRAM. If you have a 133 MHz motherboard, you need 133 MHz SDRAM.



**TIP**

For a 100 MHz motherboard, purchase 100 MHz memory, which is typically labeled *PC100*. Be aware, however, that there is some flexibility when purchasing SDRAM. For example, if when upgrading memory on a 100 MHz motherboard you can't find PC100 memory because PC133 (which is SDRAM that runs at 133 MHz) is the popular memory right now, you can run the faster memory (133 MHz) on your 100 MHz motherboard, but know that it will only run at the speed of the board.

## ***Rambus DRAM***

When SDRAM was popular, a high-speed flavor of DRAM was on the market — *rambus DRAM* (RDRAM) — which runs at speeds around 800 MHz! RDRAM chips have a 16-bit internal bus width and are packaged together in a 184-pin, gold-plated memory module called a *rambus inline memory module* (RIMM). To take advantage of this type of memory, you need a motherboard and chipset that support RDRAM. Due to the cost of RDRAM, it lost the popularity contest to SDRAM and eventually DDR memory.

## ***DDR***

*Double data rate* (DDR) memory gets its name from the fact that it can transfer data twice during each clock cycle, compared with SDRAM that can transfer data only once per clock cycle. DDR memory ships in 184-pin DIMM modules (see the section “[DIMMs](#),” later in this chapter) for desktop computers and 200-pin SODIMMs for laptop systems.

DDR memory speed is measured in MHz, like SDRAM is, and is labeled to indicate the speed. DDR memory labeling might look obscure at first because it also indicates the bandwidth by taking the speed and multiplying it by 8 bytes of data (64 bits). Here's how to read DDR memory labeled as PC-1600: Divide the 1600 by 8 bytes to get the speed of the memory. In this case, you are looking at 200 MHz memory. PC-2700 runs at 333 MHz, and PC-3200 runs at 400 MHz. When you upgrade

memory on systems that require DDR memory, you need to know the speed of the DDR memory.

Different RAM speeds for DDR memory are:

- » PC-1600 (200 MHz)
- » PC-2100 (266 MHz)
- » PC-2400 (300 MHz)
- » PC-2700 (333 MHz)
- » PC-3200 (400 MHz)

## ***DDR2 and DDR3***

Improvements to DDR memory have already started with DDR2 memory, which runs at speeds 400 MHz and higher, where DDR memory left off. DDR2 memory uses 240-pin memory modules and runs at 1.8 volts (V), as opposed to 2.5V for DDR memory. This results in less power consumption for more memory, which is great for laptop users.

Popular modules of DDR2 memory are:

- » PC2-3200 (400 MHz)
- » PC2-4200 (533 MHz)
- » PC2-5300 (666 MHz)
- » PC2-6400 (800 MHz)

DDR3 offers twice the data rate of DDR2 memory. One of the goals of DDR3 memory is to reduce power consumption; reportedly, DDR3 memory reduces power consumption by about 30 percent. DDR3 has a maximum capacity for a single DIMM module of 16GB.

Common speeds of DDR3 are:

- » PC3-6400 (800 MHz)
- » PC3-8500 (1066 MHz)
- » PC3-10600(1333 MHz)



## » PC3-12800 (1600 MHz)

DDR memory modules are 240-pin DIMMs for desktop PCs and 204-pin SODIMMs for laptop systems. (Read more on DIMMs and SODIMMs in the next section.) Like DDR2, DDR3 memory is advertised by the speed and transfer rate. For example, DDR3-800 (also known as PC3-6400) is 800 MHz memory that has a throughput of 6400 MBps. DDR3-1066 (also known as PC3-8500) memory has a throughput of 8533 MBps. Another example is DDR3-1600, which is 1600 MHz memory with a transfer rate of 12,800 MBps.

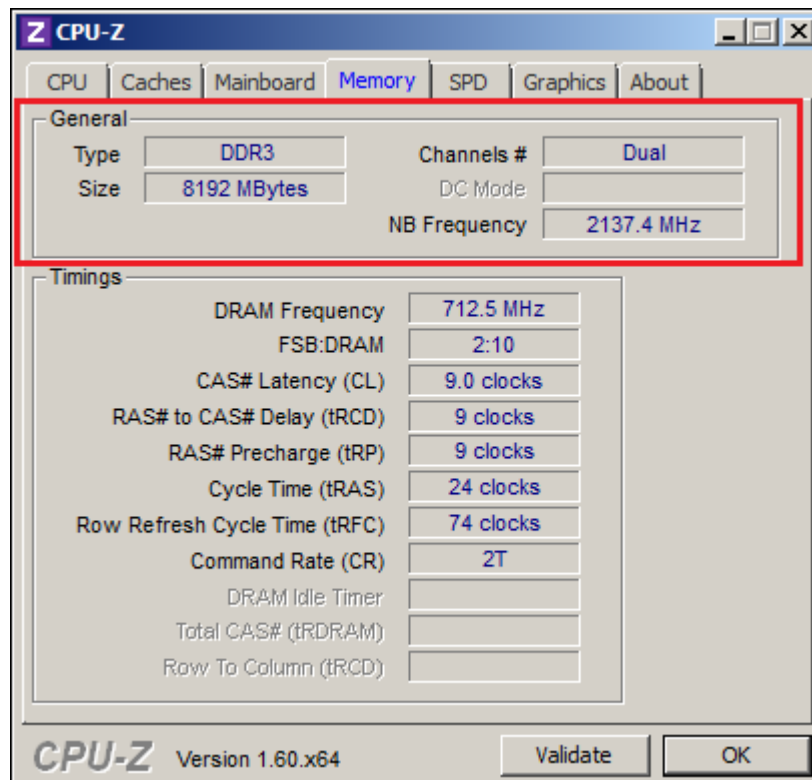
## *DDR4*

The newest form of DDR memory is known as DDR4. DDR4 improves upon DDR3 with better transfer rates and a maximum capacity per DIMM module of 64GB (as opposed to DDR3's 16GB modules).

DDR4 is able to achieve higher speeds without drastic power consumption by lowering the voltage of DDR4 memory. Two examples of DDR4 memory are DDR4-1600 (800 MHz) and DDR4-4266 (2133 MHz).

## *Viewing memory type with CPU-Z*

You can use a program known as CPU-Z to view the details on the type of memory on a system. Download CPU-Z from [www.cpuid.com/cpuz.php](http://www.cpuid.com/cpuz.php) and then run it on your system. [Figure 3-2](#) shows that when I choose the Memory tab, I see the details on the type of memory installed in my system.



**FIGURE 3-2:** Viewing memory type with CPU-Z.

## *How Would You Like Your Chips Packaged?*

Whether you are purchasing or installing RAM, understanding the different types of memory packages available is important. The following sections identify different memory packages used in desktop computers and laptop systems.

### ***DIMMs***

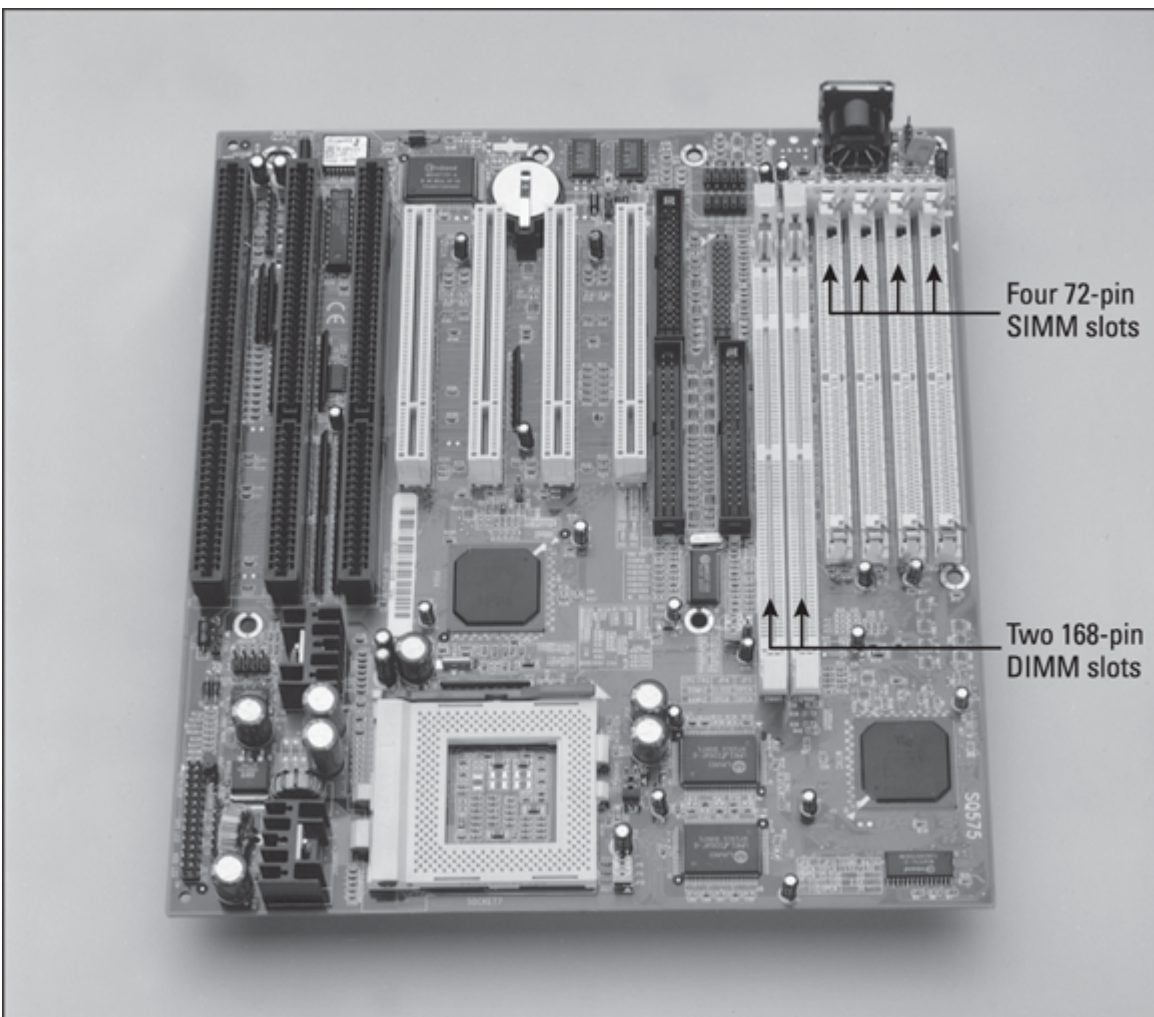
*Dual inline memory modules* (DIMMs) are how we package and install memory today. A *DIMM* card holds a number of memory chips and has an edge connector containing a number of pins that make contact with the motherboard. This design makes it quite a bit easier to install memory than it was many years ago. In the past, you had to take a dual inline package (DIP) chip out of the system board and reinsert a new chip.

Today, you purchase a card of chips (a DIMM) and install the DIMM into one of the DIMM sockets.

DIMMs supply information in 64-bit chunks. When installing memory into a system, you *must* install enough DIMMs to fill a memory bank, which is the number of DIMMs it takes to fill the data path of the processor.

Because DIMMs are 64-bit modules, and the processors today are 64-bit, you only need to install one DIMM to fill a bank.

DIMMs come in different flavors that have a different number of pins on the modules. Older DIMMs use 168 pins for SDRAM and 184 pins for DDR memory, and newer DIMMs use 240 pin modules for DDR2 and DDR3 memory. DIMM modules and sockets are shown in [Figure 3-3](#).



**FIGURE 3-3:** Looking at memory sockets on a motherboard.

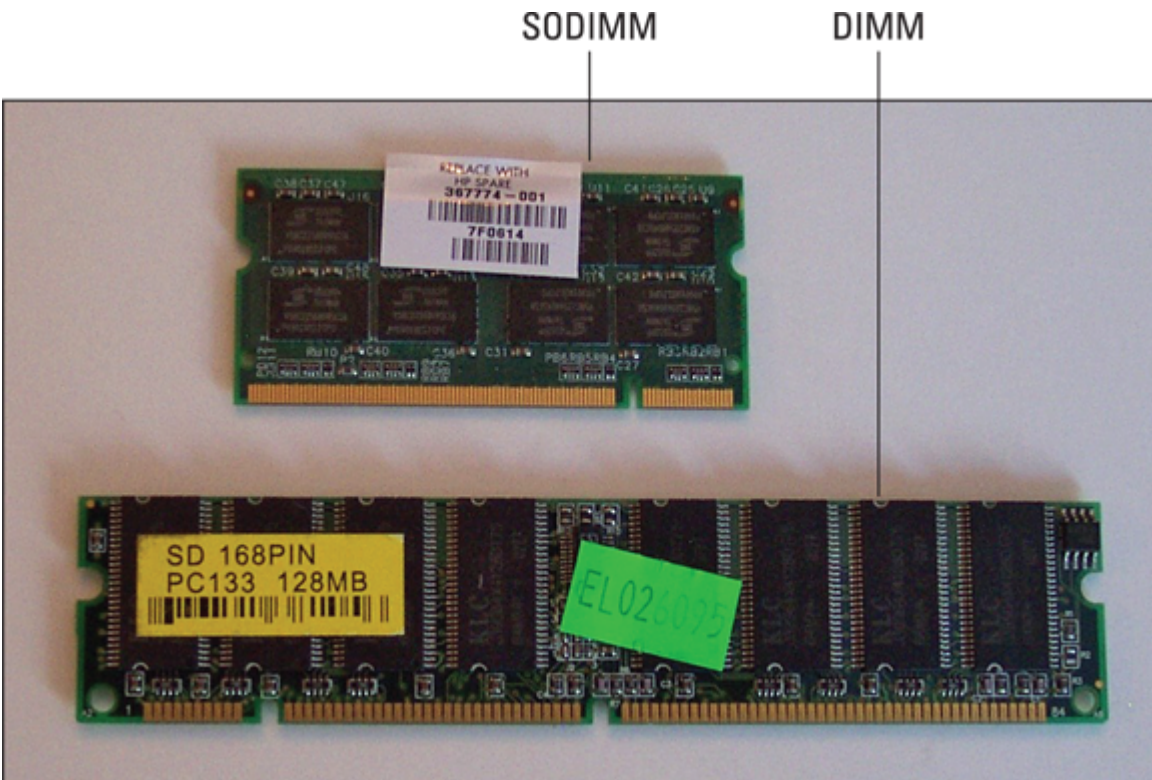


FOR THE  
EXAM

The original DIMMs were 168 pins. DDR DIMMs come with 184 pins, and DDR2 and DDR3 DIMMs use 240-pin modules. DIMMs are also the most popular type of memory module that you will find in systems today, so they should be your focus when preparing for the A+ exams.

## ***SODIMM***

*Small outline dual inline memory modules* (SODIMMs) are memory modules that are smaller than normal DIMMs and are used in laptops. A SODIMM comes in three different-sized modules: a 32-bit 72-pin module; a 64-bit 144-pin module (SDRAM); and a 64-bit 200-pin module for DDR and DDR2 laptop memory. [Figure 3-4](#) compares a SODIMM and a DIMM.



**FIGURE 3-4:** Comparing a SODIMM and a DIMM.

## *MicroDIMM*

A *micro dual inline memory module* (MicroDIMM) is another memory module used in laptop computers. The MicroDIMM is smaller than the SODIMM and comes in a 144-pin module for SDRAM and a 172-pin module for DDR memory.

# *Understanding Error-Checking Memory*

Two primary types of error-checking memory have been used in systems over the years. The following sections introduce you to these two types of error-checking memory. Be sure to become familiar with them for the A+ exams.

## *Parity versus nonparity*

*Parity memory* is a type of error-checking memory, which is memory that verifies the information stored in memory is what is actually read from memory at a later time. *Nonparity memory*, comparatively, is memory that does not perform any kind of error checking to ensure that the data written to memory is what is actually read when it is retrieved.

Here's how parity memory works. The two types of parity memory are odd and even. Both parity methods function the same way but differ in the sense of whether they look for an odd number of bits or an even number of bits. This discussion uses odd parity as the example.

With parity memory, for every byte (8 bits) of data written to memory, there is an additional ninth bit — the parity bit. When storing information to memory, the number of the enabled data bits (bits set to 1) written to memory are added up.

With odd parity, if an even number of data bits are enabled, the parity bit is set to 1 (enabled) so that there is an odd number of enabled bits in total written to memory. If the result of all the enabled data bits is odd, the parity bit is set to 0 (disabled) so that the odd number of enabled bits is retained.

After the parity bit has been set, the byte of data and the parity bit are written to memory. Even parity works the same way except that it looks for an even number of enabled bits; if the number of enabled bits is odd, the parity bit is enabled.

When the CPU requests data from memory, the data byte is retrieved along with the parity bit that was generated when the byte of information was stored in memory. The system looks at the data byte and calculates whether the parity bit stored in memory should be set to 1 or 0. It then compares the answer it has just generated with the value of the parity bit stored in memory. If the two match, the integrity of the information in memory is considered okay, the parity bit is stripped from the data byte, and the data is delivered to the CPU. If the two differ, you have a *parity error*, meaning that there is a problem with the integrity of the data stored in memory.



**REMEMBER** Parity memory cannot correct the error; it just reports that an error exists.



**FOR THE  
EXAM**

Remember that a parity error indicates something wrong with the integrity of data stored in memory.

## ***ECC versus non-ECC memory***

*Error-checking and correction* (ECC) memory is memory that can detect data integrity problems the way that parity memory can. (See the preceding section.) The difference between the two is that ECC memory can recover from the error and attempt to fix the problem with the data being read, whereas parity memory cannot. Memory that does not have ECC features is known as *non-ECC memory* as there are no error-checking and correction capabilities.

# *Multichannel Memory Architecture*

The memory architecture in a system may depend on its age:

- » Older systems only used a *single-channel* memory configuration. A *single-channel configuration* mandates a “single lane” used to send and receive information from memory.
- » When installing memory today, your system may support methods to increase memory throughput by using multiple channels.

## *Dual channel*

With some of today’s systems, though, you can install memory in a *dual-channel configuration*, which allows for two 64-bit lanes to carry information to and from memory at the same time — resulting in better performance, as the amount of data sent at one time is doubled compared to that on a single-channel architecture. This configuration increases overall performance by allowing for more input/output per operation, or clock cycle.

To take advantage of dual-channel memory, you first need to ensure that your motherboard supports dual channel, as dual-channel memory is a function of the memory controller. You also need to be using DDR, DDR2, or DDR3 memory to take advantage of dual-channel architecture. If your motherboard supports dual-channel memory, you will install the memory modules in pairs. These pairs must be similar modules in capacity and speed. For example, when installing 4GB of RAM, you install two 2GB modules. When you install these modules, install them into the same color slots on the motherboard, usually colored either black or blue. If the motherboard does not color-code the memory slots, you install the pair of memory modules in the odd-numbered slots or the even-numbered slots — but not an odd and an even.





**REMEMBER** To leverage dual channel memory, you must install the same memory modules in pairs. You must use the same type (for example, DDR2 or DDR3) of memory for both modules, the same speed, and the same capacity. The two modules must be similar because they need to be able to keep up with one another when performing parallel IO.

## *Triple and quadruple channel*

Some systems today are supporting these architectures:

- » *Triple-channel* memory architecture allows three 64-bit lanes.  
For example, Intel's i7-900 series processors support triple-channel memory architectures.
- » *Quadruple-channel* memory architecture allows four 64-bit lanes.  
The AMD G34 platform and the Intel LGA 2011 platform are examples of quadruple-channel memory architectures.

The same rules as dual channel memory apply when using triple and quadruple channel memory architectures: You must use similar memory modules, but you will be required to install either three modules (for triple-channel) or four modules (for quadruple-channel) at a time.



**TECHNICAL STUFF** With both triple and quadruple channel architectures, if you only install a pair of modules, the system will run the memory in a dual-channel architecture.

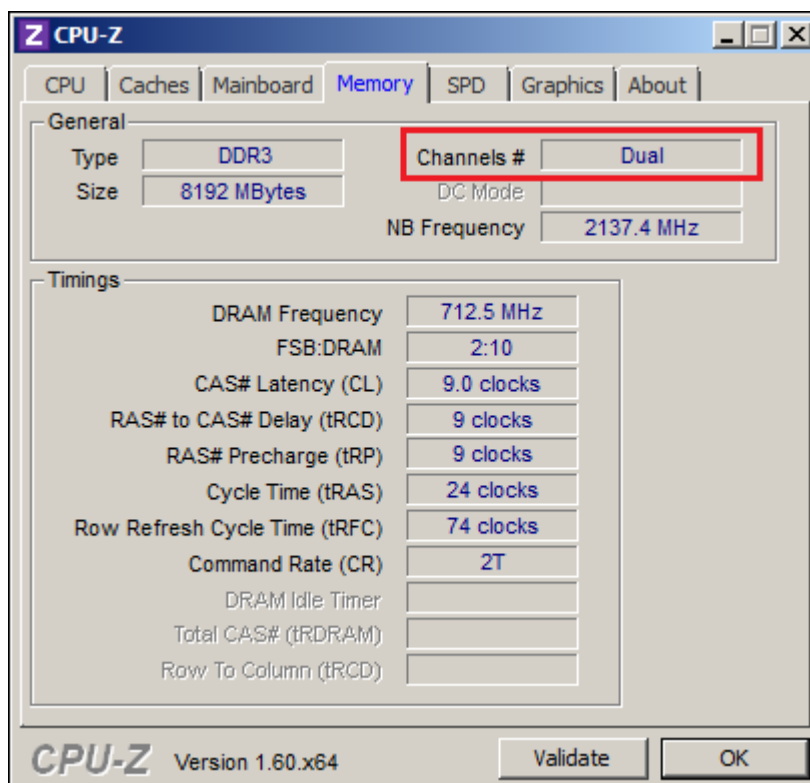




TECHNICAL  
STUFF

You can purchase dual-channel or triple-channel memory kits to ensure that you are using the same type of memory and the same speed. You do not need to use these kits, but you are paying for the fact that someone has already tested the memory in a dual-channel configuration. Some benchmarks report that you can achieve a 65 percent increase in memory performance by using a multichannel configuration.

You can use CPU-Z to check to see whether you are running your memory in a single-channel, dual-channel, or triple-channel configuration (see [Figure 3-5](#)).



**FIGURE 3-5:** Using CPU-Z to view memory channels.

# *Single-Sided versus Double-Sided Memory*

Memory modules are either single-sided or double-sided memory modules, but this characteristic does not mean that the memory chips exist on only one side of the memory card or both sides of the memory card (which is what most people think).

For *single-sided memory*, all the memory on the memory module is accessed at once by the system and is treated as a single “bank” of memory. It is important to note that the memory chips on a single-sided memory module may exist on both sides of the memory board.

For double-sided memory, the memory module (or memory board) is divided into two discrete chunks of memory (banks). The system can access only one bank at a time.



TECHNICAL  
STUFF

Original double-sided memory modules were created by taking two single-sided memory modules and connecting them.

# *Buffered versus Unbuffered Memory*

When purchasing servers (a high-end system that provides services to the entire company) for an organization, you may come across the term *buffered* and *unbuffered* memory. Buffered memory, also known as *registered*, is memory that contains registers that are used to store data before sending it to the CPU. This stored data is retained for an extra clock cycle to act as a reliability feature. Buffered memory is typically found in network servers because they have many memory modules putting stress on the system where the extra reliability is needed.

Unbuffered memory is memory that does not have registers to store information and, as a result, the memory is not as reliable. The benefit of unbuffered memory is that it has less overhead (because it is not taking time to store information in registers) and therefore, it is faster memory than buffered memory.

## *Working with Cache Memory*

*Cache memory* stores frequently used data and program code after it is read from slower DRAM. Cache memory is made up of SRAM, which is much faster than DRAM. The average speed of DRAM in the past was 60 ns, whereas the average speed of SRAM at the same time was 20 ns. If at all possible, you want the CPU's request for information to be serviced by cache memory for a quicker response. To help service these responses, the system has different levels of cache memory: L1, L2, and now L3 cache, which is common on systems today.

### *L1 cache*

Originally, *Level 1 (L1) cache* meant “internal cache” integrated into the CPU. This memory is typically a small amount of SRAM integrated into the processor's chip, giving the processor instant access to this memory with no wait time. *Wait time* is how long it takes between when the processor requests information stored in memory and it actually receives that information.

Every pre-Pentium processor had L1 cache integrated into the processor chip, but the amount of L1 cache can vary. For example, the old 486 chips had 8K of L1 cache, whereas the original Pentium processors had 16K of L1 cache. Processors today have doubled that amount to 32K of L1 cache.

The L1 cache is typically divided into two parts:

- » Half the cache is used to store frequently accessed program *instructions*.
- » The other half of the cache stores frequently accessed program *data*.

## *L2 cache*

*Level 2 (L2) cache* exists outside the CPU, usually on the motherboard or just outside the processor but in the processor casing. Therefore, some delay occurs when the processor accesses the information in L2 cache because of the distance between the processor and the L2 cache.



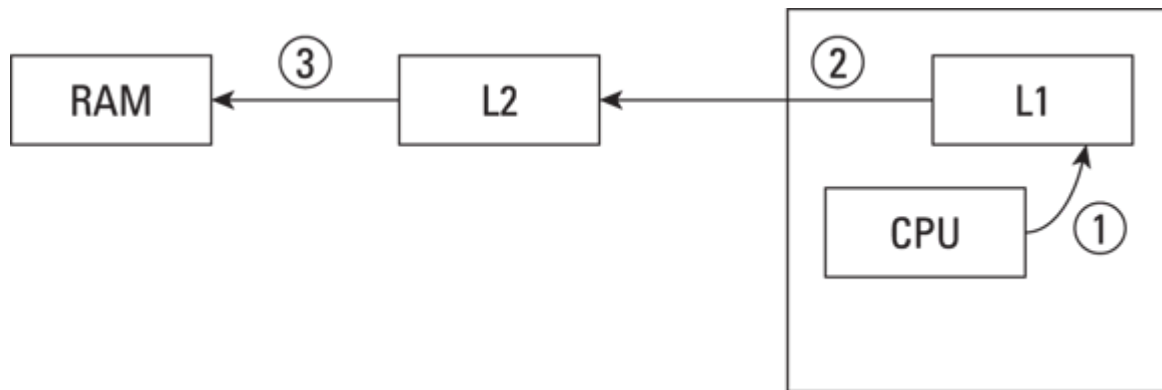
FOR THE  
EXAM

Originally, L1 cache was SRAM integrated into the processor's chip, whereas L2 cache was SRAM located outside the CPU, on the system board. Today's systems have L1 and L2 integrated into the CPU.

One of the selling points of different processors is the amount of cache memory that comes with the processor. Many processors today typically have at least 32K of L1 cache and 512K, 1MB, 2MB, or more of L2 cache inside the casing of the processor. My Intel i7 system has 128 KB of L1 cache and 2 MB of L2 cache. The more cache memory a system has, the bigger the bucket to store more frequently used information.

Figure 3-6 shows the steps the processor takes to retrieve information:

1. When the processor retrieves information, it checks whether the information is stored in L1 cache (because L1 cache has no wait time).
2. If the processor does not find the information in L1 cache, it checks the next level — L2 cache.
3. If the information cannot be found in either L1 or L2 cache, the processor finally retrieves the information from system RAM.



**FIGURE 3-6:** How the CPU retrieves information from memory.

## *L3 cache*

Because processors today provide a small amount of L1 cache *and* a large amount of L2 cache, the term *L3 cache* was used originally to identify cache that resides on the motherboard.

Today's processors are now marketing a third level of cache, known as L3, which is cache memory that resides on the processor that is shared between each processor core. This means that each core typically has its own L1 and L2 cache, while they share a larger amount (usually 6 to 8 MB) of L3 cache!

## *Viewing cache memory with CPU-Z*

You can use the CPU-Z program to view the details on the type of cache memory that is present on the system. [Figure 3-7](#) shows that I have the following types of cache on my system:

- » 32 KB of L1 cache for program data (shown as D-cache).

The *x4* means times the 4 cores on my system. This means that each core has 32 KB of L1 cache for program data.

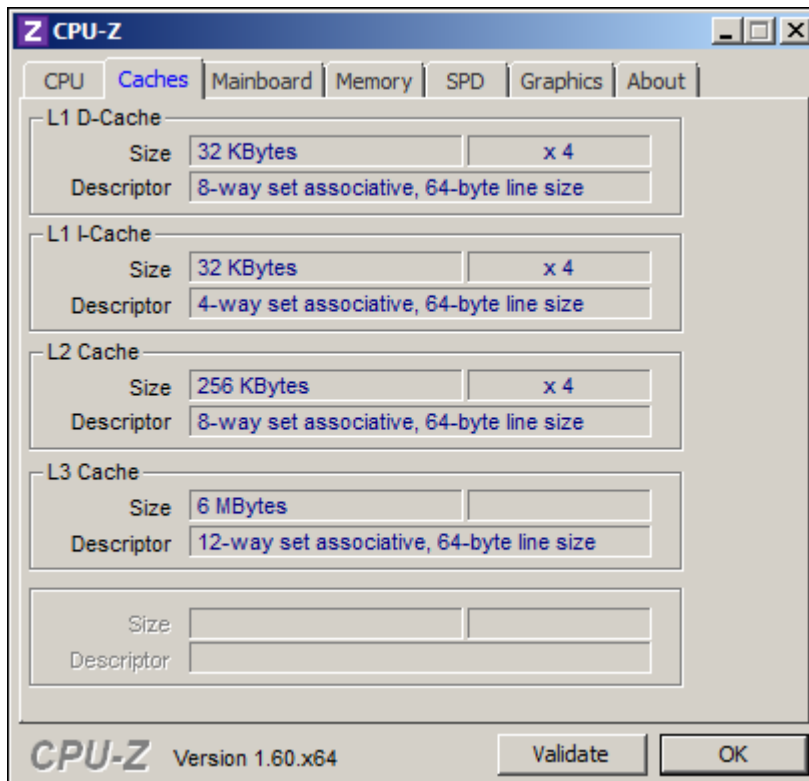
- » 32 KB of L1 cache for program instruction (shown as I-cache).

The *x4* means times the 4 cores on my system. This means that each core has 32 KB of L1 cache for program instruction.

- » 256 KB of L2 cache per processor core.

I have 4 cores on the system (denoted with a *x4*).

- » 6MB of L3 cache. Notice this is not x4, so it therefore is shared cache for all the cores.



**FIGURE 3-7:** Viewing cache memory configuration.

## *Installing or Upgrading Memory*

The discussion in this section focuses on issues related to memory upgrades. In general, upgrading memory is a simple task — assuming you purchase the proper type of memory for the upgrade. Factors that affect the proper type of memory are

- » Type of memory (FPM, EDO, SDRAM, DDR)
- » The speed of the memory
- » Pin connector type
- » Parity versus nonparity

The following sections discuss each of the factors that affect how you upgrade your system's memory. Each of these factors contributes to the compatibility of the memory being installed in your system. In order for the memory to be compatible with your system you must

- » Install the correct type of memory.
- » Use the correct memory speed.
- » Install the memory in the correct configuration used by the system.

## *Type of memory*

The first thing you need to know to upgrade your computer's memory is which type of memory you need. You need to figure out whether you need to install a DIMM, MicroDIMM, or SODIMM. Desktop computers usually need a DIMM, while laptops use a MicroDIMM or SODIMM.

After you determine the memory module type, you need to determine the type of memory to install, such as DDR, DDR2, or DDR3 memory.

## *Speed*

When you buy memory, you need to take into account the speed of the memory. Older memory, such as FPM or EDO memory, is typically measured in nanoseconds (ns) and ranges from 60 ns to 80 ns. With these types of memory, it is important not to mix speeds lest the system become unreliable. The speed of a SIMM is usually indicated on the chips themselves (displaying either a numeric value or a simple minus sign with a number). For example, a memory module running at 70 ns would show either 70 or -7 on the chips.

The speed of newer memory types, such as DIMMs and SODIMMs, is measured in MHz. When buying SDRAM or DDR memory, make sure to verify that you get the correct memory speed. For example, I recently upgraded the memory in the laptop I'm using to write this book. When I went to the store to buy a memory module, the first questions the in-store computer geeks asked were, "What type of memory?" and "What speed?" The system documentation or the CPU-Z program can help you determine

the speed of memory needed. If you don't have the documentation, be sure to look up the information on the manufacturer's website.

## Connectors

Another important issue with regard to memory installation is with the metal used on the memory modules. You need to purchase memory modules that use pins plated with the same metal used in the memory socket on the motherboard. Memory modules use silver- or gold-plated pins. If the SIMM socket, for example, uses silver-plated connectors, the memory module you purchase must use silver-plated pins. If you mix metal types, you will eventually have an unstable system.



**WARNING** Today's preferred memory modules are gold-plated DIMM modules. Do not assume that you are using gold-plated DIMMs. Always ensure that you are installing the correct type of memory by checking the documentation for your system.

## Using parity or nonparity?

The final issue with regard to memory upgrades is whether the system uses parity or nonparity memory. This information can be determined by checking the documentation that came with the system or by checking the system summary in CMOS. If you cannot find the information in CMOS or you misplace the documentation, try to find the information on the Internet at the vendor's website. When you locate the information, use [Table 3-1](#) to record the type of memory your system has so that you may refer to this when you perform a memory upgrade.

**TABLE 3-1 Identifying Memory Used by Your System**

<i>Memory Type</i>	<i>Your System</i>
Memory Type (SDRAM, DDR, DDR2, DDR3)	
Memory Speed (60 ns, 100MHz, 200MHz, 800MHz)	
Gold or Silver pins	



<i>Memory Type</i>	<i>Your System</i>
DIMM, MicroDIMM, or SODIMM	

## *RAM compatibility*

When installing memory, it is important to be familiar with RAM compatibility for the system. You need to ensure that you are installing the correct type of memory: SDRAM, DDR, DDR2, or DDR3. Also, be aware of the speed of memory your system takes. When adding memory to a system, faster memory is compatible with slower memory (as long as the type of memory is the same), but the downfall is that the faster memory will run at the lower speed if used.

## *Installing memory on desktop PCs*

After you purchase the correct type of memory — meaning the correct type at the correct speed with the correct number of pins — you are ready to install the memory.

Take off the computer's cover. You should see the DIMM slots on the motherboard, which are typically colored blue or black. Lightly, but firmly, place the DIMM in the socket and then push down and clamp either end in place with the clips available. Note that when you install the memory module, the memory module can only go in one way, as there are grooves in the slot that the module has to sit in properly.



ON THE  
WEB

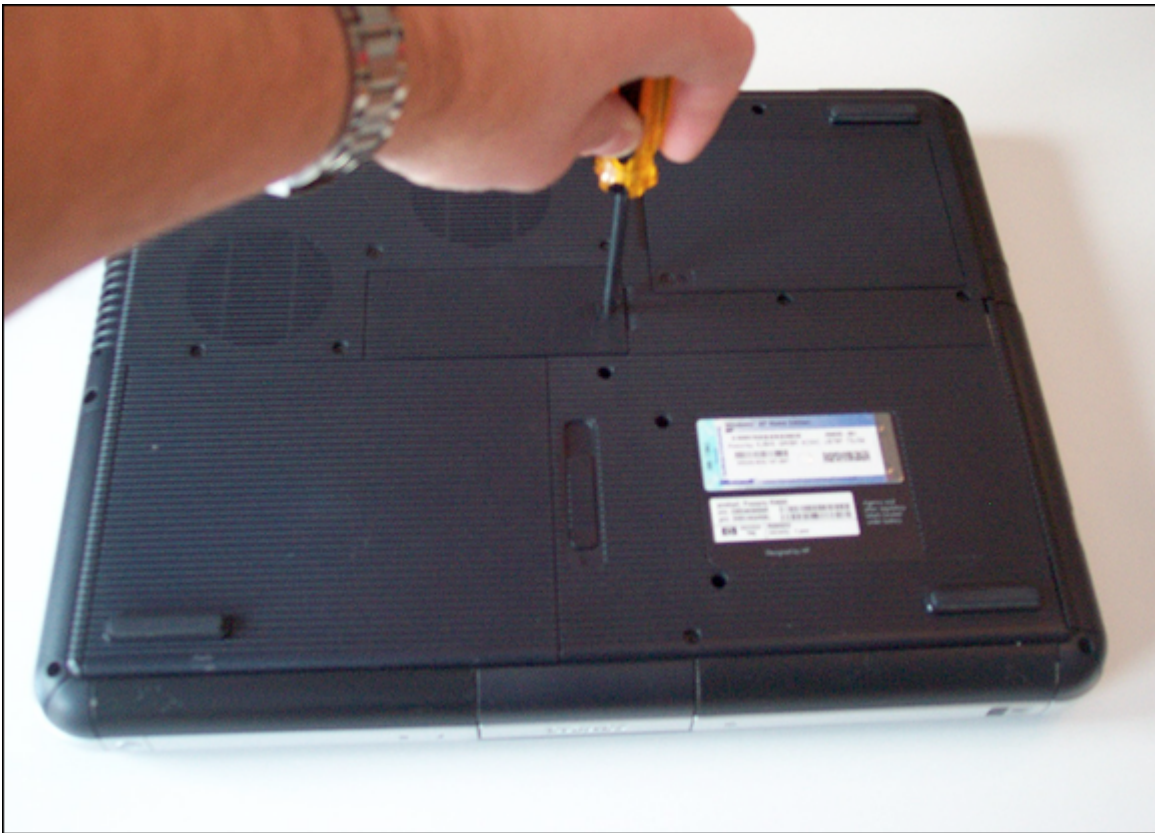
Lab 3-1 and Lab 3-2 can be downloaded from the book's companion website: [www.dummies.com/go/aplusaio](http://www.dummies.com/go/aplusaio). Use Lab 3-1 to practice finding out what type of memory you have; Lab 3-2 gives you practice installing memory on a desktop system.

## *Installing memory on laptop systems*

Installing memory on today's laptop systems is just as easy as installing memory on a desktop PC. The first step is to make sure you buy the

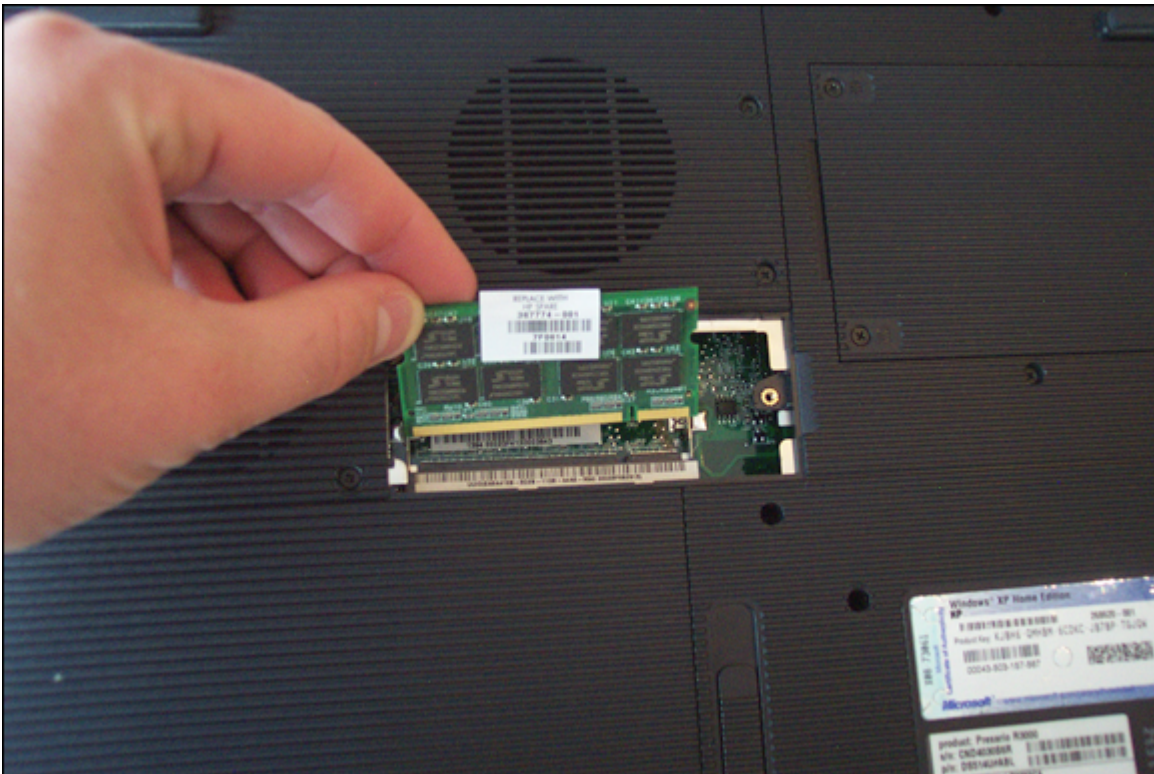
correct type of memory for the laptop. Again, check the laptop documentation before heading to the store!

To install your memory, flip the laptop over. You'll notice a door on the bottom of the laptop that can be removed (shown in [Figure 3-8](#)). This is where you add memory.



**FIGURE 3-8:** Remove the cover to add memory to a laptop.

After the cover is removed, you can insert the SODIMM into an empty slot by lightly placing the SODIMM into the memory slot on a slight angle and then clamping it back into place, as shown in [Figure 3-9](#). If you are replacing memory, first remove the old memory module by pressing the clips on the side and then lifting out the old memory.



**FIGURE 3-9:** Inserting the SODIMM module into the memory slot.

When you have the SODIMM locked in place, put the cover back on.



**ON THE  
WEB**

Use Lab 3-3 for practice finding out what type of memory is needed by a specific laptop. In this lab, you research the laptop on the Internet. Lab 3-3 can be downloaded from the book's companion website: [www.dummies.com/go/aplusaio](http://www.dummies.com/go/aplusaio).

## Getting an A+

This chapter provides an overview of the different types of memory and installation of memory. I touched on the following points:

- » *Read-only memory* (ROM) is memory that can be read from but not written to, and the information stored there is permanent.

- » *Random access memory (RAM)* is volatile memory that can be written to and read from; information stored there is flushed out when power is lost.
- » *Dynamic RAM (DRAM)* is memory that needs constant refreshing of its memory cells; it is also the type of memory that is typically upgraded on systems.
- » *Static RAM (SRAM)* is static memory, meaning that it does not need refreshing as often as DRAM does. SRAM is also faster than DRAM. SRAM is typically used for cache memory.
- » Today's systems have *L1 and L2 cache* unique to each processor core. A large amount of *L3 cache* is built into the processor that is shared between processor cores.
- » Memory is installed with *memory modules*. Whereas 72-pin SIMMs were popular in original Pentium systems, DIMMs are now the popular memory module for desktop systems. Laptops use SODIMMs as their memory module type.
- » You need to know the *type of memory* your system uses before you upgrade your system. For example, you need to note whether your system uses SDRAM or DDR memory. Also be sure to note the speed of the memory.

## *Prep Test*

- 1. Which of the following types of memory is used for cache memory?**
  - (A) SRAM
  - (B) DRAM
  - (C) EDO RAM
  - (D) SDRAM
  
- 2. You are a technician for a company and have been asked to install memory in a dual-channel configuration. Which of the following types of RAM can be installed?**

- (A) SDRAM
- (B) DIMM
- (C) Rambus
- (D) DDR

**3. You are assessing a system and trying to locate the cache memory. Where does the Level 1 (L1) cache reside?**

- (A) Motherboard
- (B) Video card
- (C) CPU
- (D) BIOS

**4. You are a technician for your company and you have been asked to upgrade the RAM on a salesperson's laptop. What type of memory module will you install? (Select two.)**

- (A) DIMM
- (B) SODIMM
- (C) DRAM
- (D) L1 cache
- (E) MicroDIMM

**5. Your manager is looking for memory that can protect against data corruption in the memory module. What feature is she looking for in her memory?**

- (A) ECC
- (B) Parity
- (C) Nonparity
- (D) Dual channel

**6. You are a technician for your company and have been asked by management to upgrade the RAM from 4GB to 8GB in all the desktop systems within the accounting department. You have**

**purchased a number of DDR3 memory modules. Some of the desktops are currently running DDR2 and others are running DDR3. Which of the following represents the outcome of the upgrade?**

- (A) The DDR2 desktops can use the new DDR3 memory as long as the DDR3 modules are installed in the first slot.
- (B) The DDR2 desktops can use the new DDR3 memory as long as the DDR3 modules are installed in the last slot.
- (C) The DDR2 desktops can be upgraded as long as you alternate between the slots using DDR2 and DDR3 memory modules.
- (D) The desktops using DDR3 are the only systems that can be upgraded.

**7. How many pins does a DIMM have? (Select all that apply.)**

- (A) 64
- (B) 128
- (C) 168
- (D) 32
- (E) 184
- (F) 196
- (G) 240

**8. You are upgrading the RAM on a desktop system and need to install RAM that is compatible with PC2-5300. Which of the following are compatible and would maintain the performance of the desktop?**

- (A) PC2-3200
- (B) PC-2400
- (C) PC3-6400
- (D) PC2-6400

**9. If memory data is corrupted, what type of error is created?**

- (A) File access error

- (B) Parity error
- (C) Disk error
- (D) DRAM error

**10. You are a service technician for your company. Your manager has asked you to install memory in the sales manager's desktop. You notice that there are four memory slots in the desktop: Two slots are colored blue and two slots are colored black. In what configuration would you install memory in order to get the best performance?**

- (A) The slower memory should be installed in pairs within the black slots.
- (B) Memory modules of the same size and speed should be installed in pairs in either the blue or the black slots.
- (C) The slower memory should be installed in pairs within the blue slots.
- (D) Alternate between the blue and the black slots as you install each memory module.

**11. What type of memory is typically used for storing computer BIOS code?**

- (A) DRAM
- (B) SRAM
- (C) RAM
- (D) ROM

**12. You are installing two DDR2 memory modules: One is 800 MHz and the other is 600 MHz. Which of the following represents the speed at which both memory modules will run?**

- (A) 1400 MHz
- (B) 800 MHz
- (C) 600 MHz

(D) 200 MHz

**13. How many DIMMs are used to fill a memory bank in an Intel i7 system?**

(A) 1

(B) 2

(C) 3

(D) 4

## Answers

1. **A.** SRAM is used for cache memory. DRAM — known as system memory — stores data and program code that are running. EDO and SDRAM are types of DRAM. See “[SRAM](#).”
2. **D.** In order to take advantage of dual channel memory you must have a motherboard that supports it and be using DDR, DDR2, or DDR3 memory. Review “[Multichannel Memory Architecture](#).”
3. **C.** L1 cache is cache memory integrated into the CPU, while L2 cache memory was originally external to the CPU and typically located on the motherboard. Check out “[L1 cache](#).”
4. **B and E.** When installing memory in a laptop, you will use SODIMM or MicroDIMM memory modules as they are modules sized for laptops. Peruse “*How Would You Like Your Chips Packaged?*”
5. **A.** A feature of memory that allows it to fix data integrity and corruption is *Error-Checking and Correction*, or ECC memory. See “[ECC versus non-ECC memory](#).”
6. **D.** Because you have purchased DDR3 memory you can only upgrade the RAM in systems that take DDR3, which would be the systems already using DDR3 memory. The systems using DDR2 memory are not compatible with DDR3 memory. Look over “[RAM compatibility](#).”



7. **C, E, G.** DIMMs come in different flavors: 168-pin (for SDRAM), 184-pin (DDR), or 240-pin (DDR2 and DDR3) memory modules. The other choices for this question are just common numbers used in the computer field, but there are no memory modules that use those numbers of pins. *Study “[DIMMs](#). ”*
8. **D.** When upgrading RAM in a system, you need to ensure that the RAM is compatible with the existing memory. To be compatible, you must install the same type of memory of at least the same speed. You can install memory that is faster, but know that the memory will run at the lowest speed of the memory installed. *Refer to “[RAM compatibility](#). ”*
9. **B.** You’ll receive a parity error if there are any problems with data stored in memory. *Examine “[Parity versus nonparity](#). ”*
10. **B.** When installing memory in a system, try to install the memory into a dual-channel configuration to get the best performance possible. To do this, you must have two memory modules of the same speed and capacity and install those modules in slots that are paired for dual-channel configuration (either both blue slots, or both black slots). *See “[Multichannel Memory Architecture](#). ”*
11. **D.** A computer manufacturer’s BIOS/UEFI code is typically stored on read-only memory. Today’s version of the BIOS chip can be reprogrammed by running special software to update the BIOS. *Check out “[Read-only memory \(ROM\)](#). ”*
12. **C.** The memory will run at the lowest common speed between the memory modules. This means that if using a 600 MHz and an 800 MHz memory module, the speed that both modules run at is 600 MHz. *Peek at “[RAM compatibility](#). ”*
13. **A.** Pentium 4s have 64-bit data paths, and a DIMM has a 64-bit data path as well. Thus, you need only one DIMM to fill a bank in a Pentium 4 system. *Look over “[DIMMs](#). ”*

# Chapter 4

## Telling Your BIOS from Your CMOS

---

### IN THIS CHAPTER

- » Identifying the purpose of BIOS
  - » Upgrading a system BIOS
  - » Identifying the purpose of CMOS
  - » Identifying common settings contained in CMOS
- 

A big part of system configuration is understanding what CMOS is and how the different settings within CMOS can help you troubleshoot a system. A wonderful talent to have as an A+ Certified Professional is the ability to understand CMOS and its functionality. Although CMOS doesn't seem like a place where you'd need to go every day, many PC-related problems can be solved in CMOS.

In this chapter, you learn some of the common CMOS options that are found in modern systems. Keep in mind that these options might be labeled differently on your system or might not even exist on your system, as the CMOS setup program is unique to each system. For example, the CMOS setup program on a Lenovo system differs from that of a Dell even though the concept of CMOS remains the same.

I start the chapter with a discussion of the system BIOS and then compare it against CMOS; the two are closely related and are often confused by many IT professionals.

## *BIOS versus CMOS*

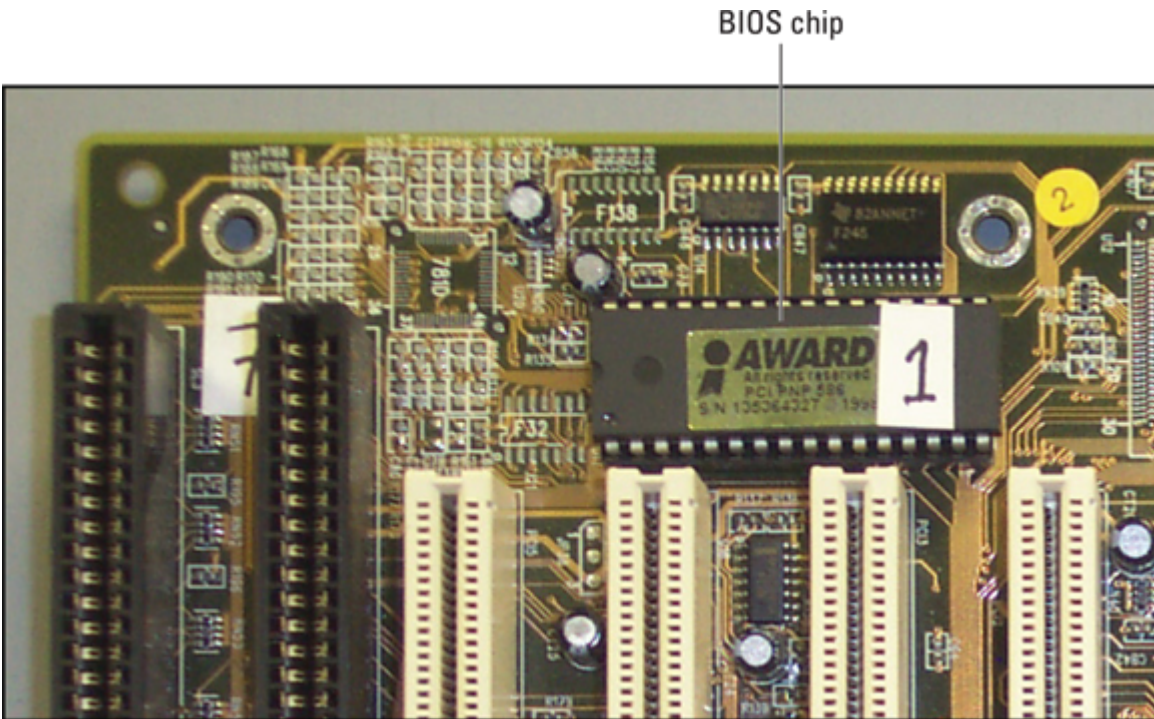


FOR THE  
EXAM

*BIOS* — basic input-output system — is the low-level instructions the system uses to communicate with the system devices. This is different than *CMOS* (complementary metal-oxide semiconductor), which is simply an inventory list of the configuration information for the system, containing information such as the hard drive space and amount of memory that exists on the system. Keep this in mind:

- » CMOS is the inventory list.
- » BIOS is the actual code that is run to communicate with those devices.

Originally, the BIOS was stored in a ROM chip on the motherboard. Because of this, you used to have to replace the entire chip with a new chip to update the BIOS. Today's systems, however, have the BIOS code stored in an EEPROM (electronically erasable programmable read-only memory) chip located on the motherboard. (For more information on ROM and EEPROM, check out the memory topic in [Chapter 3](#) of this minibook.) The chip that contains the BIOS code is called the *BIOS chip*. The BIOS chip should be easy to find — it's usually rectangular and clearly labeled, typically with the name of the manufacturer of the BIOS chip and the date when the chip was created. In [Figure 4-1](#), the BIOS chip is the chip with the white label indicated with a number 1.



**FIGURE 4-1:** The BIOS chip (an EEPROM chip located on the motherboard) contains the BIOS code.

Along with the low-level code, the BIOS also contains the POST (power-on self-test) and the CMOS setup program. The *POST* is a self-diagnostics routine that the system goes through each time it boots up. This self-diagnostic checks to see that each device listed in CMOS actually exists on the system. The POST also tests devices, such as I/O (input/output) ports and memory, to verify not only that they exist but also that they still function.

You use the CMOS setup program, which is stored in the BIOS, to navigate through the CMOS settings. However, the BIOS does not contain the settings themselves. As you find out in the upcoming section, “[Understanding CMOS](#),” the CMOS settings are maintained in CMOS RAM.

## NEW AND IMPROVED UEFI

The BIOS has been the standard firmware code, or interface, for the computer since the early days of the PC. Over the last number of years, there have been enhancements to the functionality of the BIOS in a new specification known as *Unified Extensible Firmware*

*Interface*, or UEFI. UEFI is designed to replace the older BIOS interface on newer systems and comes with a number of benefits:

- Improved security to ensure that the startup environment has not been tampered with.
- Quicker startup time when booting the PC and resuming from hibernate mode.
- Support for more partitions and larger partition sizes due to the use of the GUID partition table (more on drives in Book 2, [Chapter 5](#)).
- The UEFI setup program is more graphical and includes mouse support.
- Backward compatible with older systems by being able to run in BIOS mode.

## *Upgrading the System BIOS/UEFI*

When your system was designed, its BIOS program code was designed to work with very specific devices. As you know, computer technology changes very quickly, almost overnight. So, what can you do if you have an older system and you want to update its capabilities?

The BIOS dictates a system's capabilities. For example, assume that the BIOS on your old computer does not support virtualization (more on this later). It is possible that after you update the BIOS code your system may have virtualization support. As far as the current BIOS in your system is concerned, there is no such thing as virtualization. Thus, you need an upgraded BIOS to make the system understand!

Another example of a good time to upgrade the BIOS code in hardware is with a wireless home router. A few years back, I purchased my first wireless router. I knew that I wanted to configure the wireless network to limit which Media Access Control (MAC) addresses (network cards) could connect to the wireless network. Unfortunately, there was no such

setting in the configuration screens of the wireless router, so I went to the manufacturer's website and updated the BIOS in the router. After I completed the upgrade of the router, the setting I was looking for suddenly appeared on the configuration screens! The point is that it is extremely common to upgrade the BIOS on devices to make sure that the device is up to date with the current trends.

## ***Performing BIOS upgrades/firmware updates***

In the past, with much older systems, you would upgrade the BIOS by completely replacing the BIOS chip. Back then, BIOS was stored on a ROM (read-only memory) chip, which could not be written to. So the only way to get new BIOS code was to replace the entire chip!

Today's systems use a modified version of the ROM chip: an EEPROM chip. To upgrade the program code on an EEPROM chip, you do not need to physically replace the chip; you just run a software program that is designed to rewrite the program code.

To upgrade the BIOS, also known as the firmware, for your system, you navigate to the website for your PC, laptop, or device and then download the latest BIOS update/firmware upgrade for the system. Be sure to follow the manufacturer's directions on how to apply the update to your BIOS.

When updating your BIOS, you first go to the manufacturer's website and download the BIOS update program. After you download the BIOS update program, you then run the program on your system, and it rewrites the BIOS code on the BIOS chip. Because you are writing to this ROM chip with a special program, the ROM is called a *flash ROM*, where *flashing* is the process of rewriting the program code.

## ***Potential issues with BIOS upgrading***

If you decide to perform a BIOS upgrade, consider these few words of caution:

### **» Be sure you're applying the correct BIOS update for the system.**

You want to make sure that you are aware of the manufacturer for your BIOS before you look for an update. With this information, you can go to the manufacturer's website and download the update. You will not

be able to mix BIOS codes between manufacturers. For example, you cannot update your Compaq system with a BIOS update from Dell.

- » **Be sure that you not only have the BIOS update for the correct system, but also that the BIOS update you have is designed for your version of the BIOS.** Each BIOS has a revision number or version number. The developers of the BIOS update program might place a version check into the BIOS update, but you cannot be sure of that. So, as a result, be sure to double-check that the BIOS update you are running is for the *BIOS version* you have.



**WARNING** Installing the wrong BIOS version can cause the system to become dysfunctional. If you can't find a BIOS version number, use the BIOS date to decide which update to download. The current BIOS version or date can be located within CMOS or seen with the BIOS manufacturer on the screen during boot-up, as shown in [Figure 4-2](#).

- » **When you start a BIOS update, be sure that you complete it.** Rewriting only a portion of the BIOS code (whether as a result of an accidental shutdown or power loss during the writing process) can cause the system to become dysfunctional. The actual BIOS update should take only a few seconds, so try not to disrupt the BIOS update after it starts.

Phoenix BIOS 4.0 Release 6.0  
Copyright 1985–1998 Phoenix Technologies Ltd. All Rights Reserved  
Copyright 1996–1998 Intel Corporation.  
404CL0X0.15A.0306.P02

Intel Celeron(tm) processor 333 MHz  
128MB System RAM

Legacy Keyboard ... Detected  
Legacy Mouse ..... Detected

Fixed Disk 0: QUANTUM FIREBALL EX10.2A-(PM)  
ATAPI CD-ROM: MATSHITA CR-588-(SM)  
ATAPI Removable Drive: IOMEGA ZIP 100-(SS) ATAPI

Press <F1> to enter SETUP

**FIGURE 4-2:** Identifying the BIOS version by starting up the system.



**TIP**

As a way to prevent accidental writing to the BIOS code, some motherboards ship with a *jumper* on the board that must be removed to write to the BIOS chip. When you want to upgrade the BIOS and you have the correct BIOS update, you remove the jumper and then run the BIOS update. After updating the BIOS, you place the jumper back.

Now that you have an understanding of what the BIOS is used for and how to update the BIOS, it is time to move on to CMOS and the different computer settings that can be controlled through CMOS.

## *Understanding CMOS*



As I mention earlier, *CMOS* contains the computer's inventory list and advanced setup options. It can be considered an inventory list because it contains a record of all the devices connected to the system, such as the floppy drive, the hard drive, memory, and so on. Not only does CMOS list the devices, but it also dictates their capacity — for example, whether the system supports 2GB or 8GB of memory.

During the boot process, the system compares its inventory list with what it detects during boot-up. If there are any discrepancies, the system typically gives you an error and takes you into CMOS right away, asking you to save the new change. For example, assume that your system has 2GB of RAM and you add another 2GB of RAM. When you power up the system, the system compares what it had in inventory (2GB) the last time it booted with what it sees now (4GB). Because there is a difference, CMOS reports a memory size error and gives you the opportunity to save the new changes to CMOS. CMOS doesn't know whether the difference is for the better; it sees a difference, so it reports an error. Because CMOS detected the new memory, all you have to do is save the changes to the inventory list and reboot.



**TIP** Looking at the previous example, if you choose not to save the settings, you will get the memory size error the next time you start the computer. To prevent the error from appearing again, save the changes to CMOS. This way, the values that are detected are equal to what is stored in CMOS.

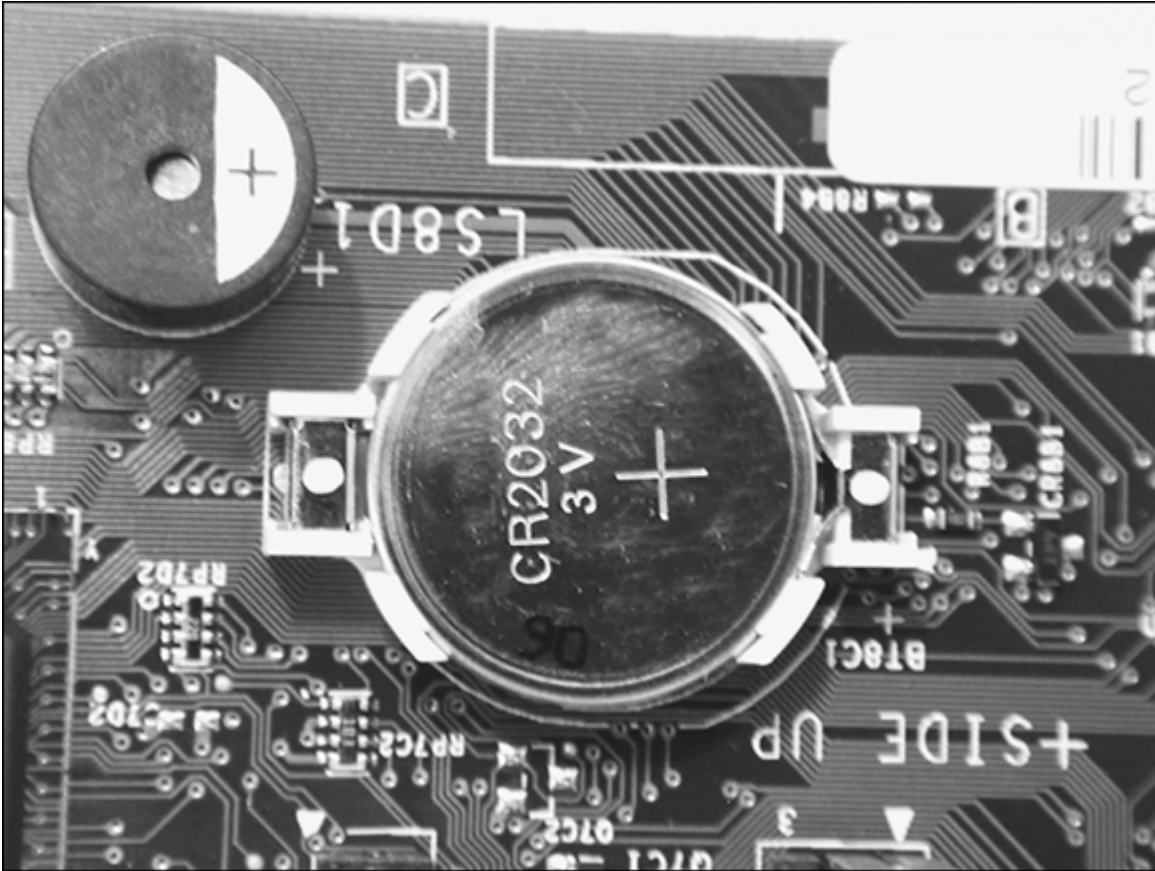
Before discussing the different CMOS settings, it's important to know how to enter the CMOS setup program. Figuring this out is difficult on some systems yet extremely easy on others. Some systems display a message on boot-up that indicates what keystroke (often Delete, F1, or F2) to use to enter the CMOS setup program. IBM systems typically use F1 (refer to [Figure 4-2](#)); Dell systems today typically use F2 or Delete, while older Compaq systems typically used F10, or sometimes F2, as is the case with my Compaq laptops. The point here is that each manufacturer may use a different keystroke to enter CMOS.

In some older systems, you enter CMOS by holding down multiple keys at the same time during boot-up — Ctrl+Alt+S or Ctrl+Alt+Insert, for example. Entering into these systems is a little trickier, so reviewing your documentation is helpful. (Note that it has been a long time since I have seen a system that uses these three-key combinations to enter the CMOS setup program.) [Table 4-1](#) summarizes popular keystrokes used to enter CMOS, based on the manufacturer of the BIOS. (Remember that the CMOS setup program is stored in BIOS.)

**[TABLE 4-1](#) How to Enter CMOS Setup**

<b><i>BIOS Manufacturer    Keystroke</i></b>	
AMI	Delete
Award	Delete or Ctrl+Alt+Esc
Acer	F2 or Delete
Compaq	F10 or F2
Dell	F2 or Delete
HP	F1
IBM	F1
Phoenix	F1 or F2

CMOS information is held in *CMOS RAM*, which is volatile memory that can maintain its data during shutdowns or power loss by using a small battery located on the motherboard. Thus, if the battery on the motherboard loses power, the CMOS data is also lost. [Figure 4-3](#) shows a CMOS battery on a system board.



**FIGURE 4-3:** The CMOS battery on the system board is responsible for powering CMOS RAM.



**FOR THE  
EXAM**

The CMOS configuration is stored in CMOS RAM. Because RAM loses its contents when the system is powered off, the motherboard has a small battery that maintains enough of a charge that CMOS RAM can maintain its data — thus allowing the system to retain the CMOS information between reboots.

## *Viewing Basic Interface Settings*

In this section, you find out about common CMOS setup options, also known as *BIOS component information*, and their purposes. These CMOS settings are consistent with most systems and have become fairly

standard settings to view or change through the CMOS setup program when troubleshooting a system.

After you enter the CMOS setup program, you may see an introductory screen, such as the one shown in [Figure 4-4](#), displaying options that can be changed, which allows you to control the system configuration.



**FIGURE 4-4:** A typical CMOS screen.

## *Hard drive*

Within the CMOS setup program, you can find the size of the hard drive. CMOS displays the size of the hard drive based on what is detected during startup. The hard drive size is displayed in CMOS, as shown in [Figure 4-5](#).



**FIGURE 4-5:** Viewing the hard drive size in CMOS.

The hard drives are typically displayed in today's systems as individual storage devices. You simply highlight the storage device and press Enter to view the details. On older EIDE/PATA systems, the drives show as primary master, primary slave, secondary master, and secondary slave. Each entry shows the label of the drive; you highlight it in CMOS and then press Enter to view the details on the drive. The details can include the size of the drive, its geometry, and any settings for the drive.

On some older systems, you could change the CMOS from autodetect to manual so that you can specify the dimensions of the drive — overriding what was detected. Specifying the dimensions of the drive involves looking on the back of the drive to find out how many sectors, cylinders, and heads the drive contains — which dictates the size of the drive. When you know the dimensions, you can input these dimensions into CMOS (after switching from autodetect to manual). CMOS calculates the size of the drive based on the dimensions you input.

On older systems, you specify the hard drive size by specifying a *drive type*, which is a number representing a drive of a specific size. For example, a Type 2 drive might be 1.2GB in size, and a Type 10 drive might be 1.5GB in size. (The actual values of hard drive types vary from system to system and are usually displayed along with the type.) There is also a custom type on older systems — usually Type 47 — which enables you to specify the dimensions of the drive (sectors, cylinders, heads); CMOS can then calculate the size in megabytes for you after you input the dimensions.

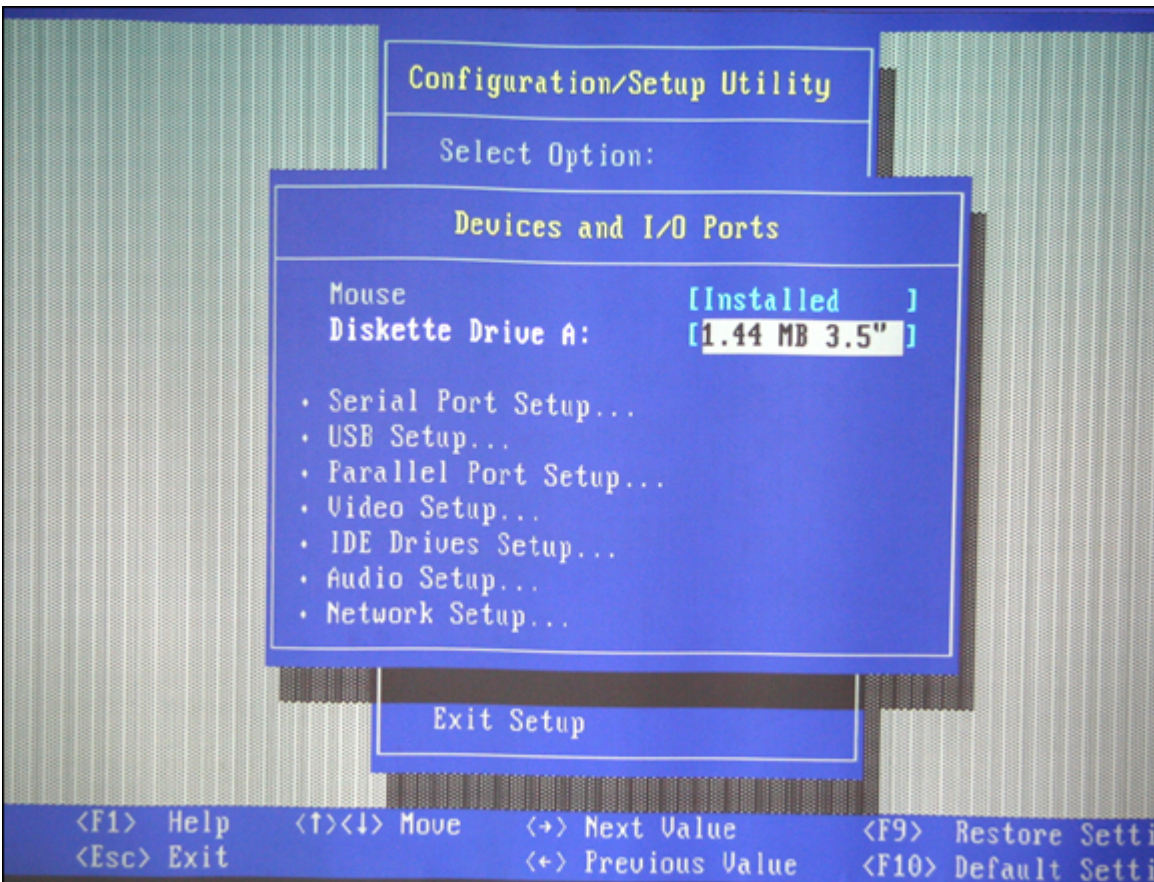
## *Optical drive*



The CMOS stores basic information related to optical drives such as CD and DVD drives that are detected in the system. These optical drives can also be specified in the boot order of CMOS to control whether your system boots from CD or DVD drives. (The boot order, also known as boot sequence, is covered later in this chapter in the section called “[Boot sequence](#).”)

### ***Floppy disk drive***

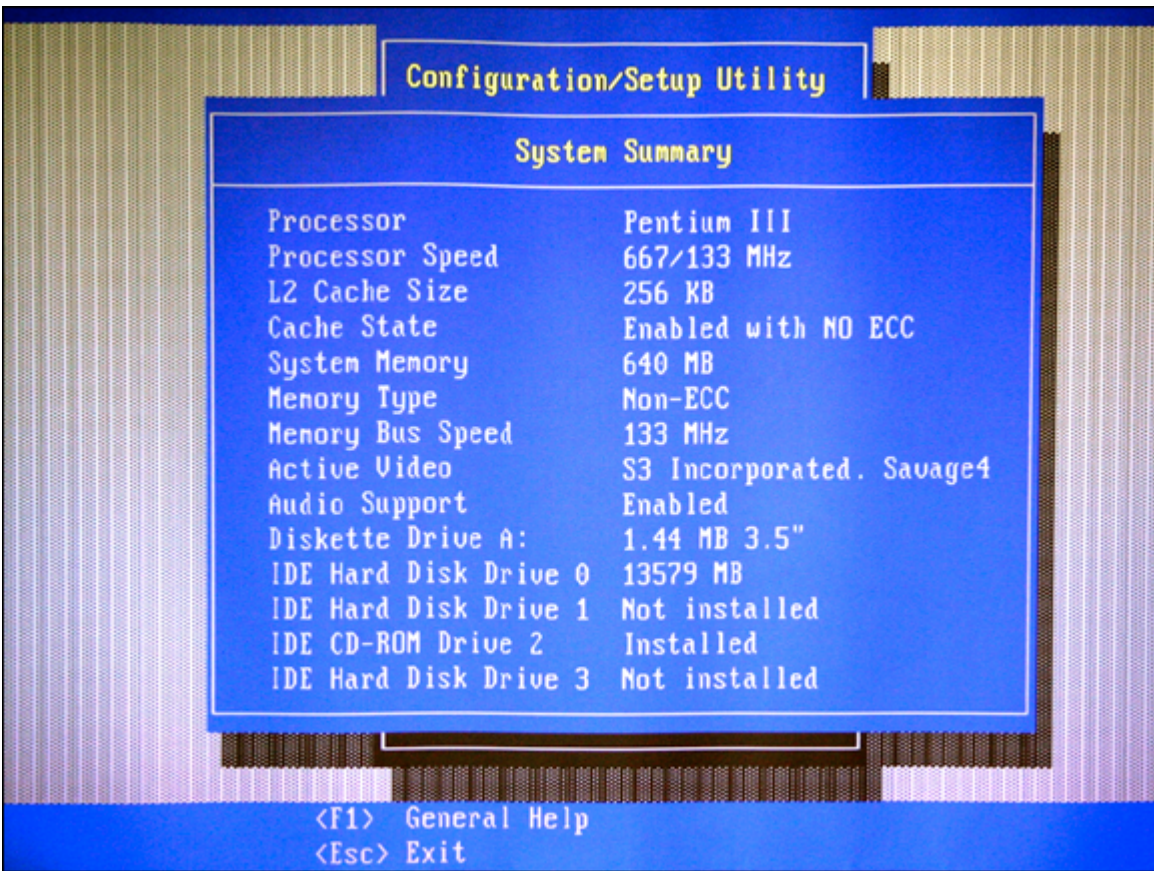
If you have an older system with a floppy drive, CMOS lets you enable or disable the floppy disk drive. When the disk drive is enabled, its size is also specified and can usually be changed. If the disk drive is enabled but the wrong size disk drive is specified, you might not be able to access a floppy disk that has been placed in the drive. CMOS allows you to disable devices such as disk drives and USB ports so that companies can keep employees from copying proprietary data. [Figure 4-6](#) shows the menu setting that allows you to change the size of the disk drive and even disable the disk drive.



**FIGURE 4-6:** Changing the size of the floppy disk drive in CMOS.

## *Memory/RAM*

CMOS indicates the total amount of memory installed on the system. Typically, this entry is not modified unless you add or remove RAM and the change is detected on boot-up. If you do add or remove RAM from the system, the system detects the change and modifies CMOS for you. All you need to do is save the modification once in the CMOS setup program. Some systems today inform you that the system has saved the change for you and don't require you to enter the CMOS setup program. [Figure 4-7](#) shows the CMOS System Summary screen, which shows that there is 640MB of system memory installed on the system.



**FIGURE 4-7:** Viewing the amount of memory installed on the system through CMOS.

The CMOS in some systems not only tells you how much memory you have installed but also informs you of the *type* of memory that is installed. Here you should be able to see whether your system is using SDRAM, DDR, DDR2, or DDR3 memory. You should also be able to see the speed of that memory within CMOS.

### ***CPU and clock speeds***

CMOS displays system information such as the type of processor found on the system and contains detailed information about that processor such as the speed of the processor (*clock speed*) and the amount of cache memory present in the processor. You may have to view the system summary information to view the CPU speed.

### ***Parallel port***

CMOS offers the opportunity to configure your parallel port. This configuration allows you to either disable the port or change the mode the



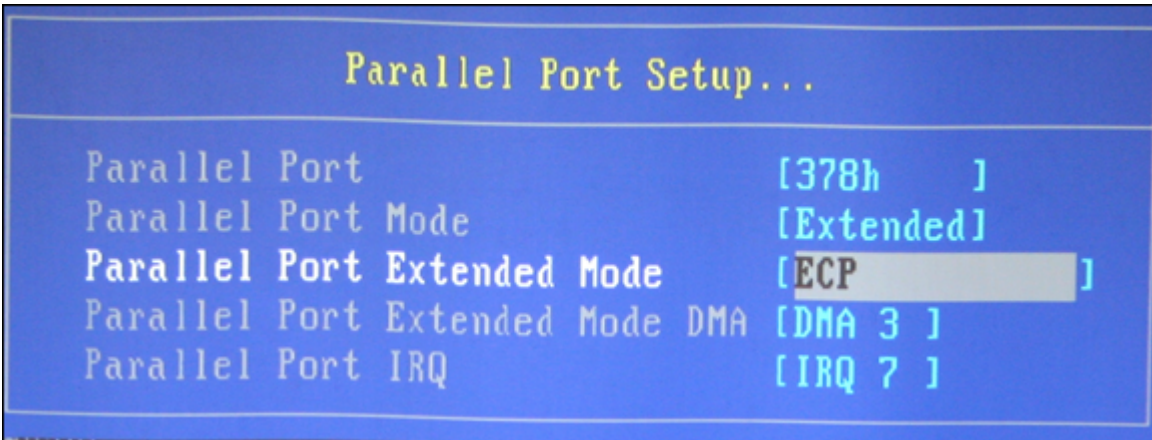
port runs in.

You might think that a parallel port does not require a lot of configuration, but think about this: Have you ever had problems with a scanner that plugs into your parallel port? Or more specifically, have you ever had problems with your parallel-port scanner plugging into your computer and the printer then connecting to your scanner? The problems might derive from the parallel port mode being misconfigured on the system. The *parallel port mode* dictates the capabilities of the parallel port. [Table 4-2](#) lists the three parallel port modes that can be configured for your system.

**[TABLE 4-2](#) Parallel Port Mode**

<b>Mode</b>	<b>Data Transfer Rate</b>	<b>Description</b>
Standard Parallel Port (SPP)	150 KBps	Supports communication in only one direction: from the computer to the device.
Enhanced Parallel Port (EPP)	2 MBps	A bidirectional port mode that enables communication in either direction: from the computer to the device and the device to the computer. This mode supports <i>daisy-chaining</i> .
Extended Capabilities Port (ECP)	More than 2 MBps	Supports bidirectional devices.

If you're having trouble daisy-chaining the scanner and printer off the parallel port on the computer, check to make sure that the proper port mode is selected in the CMOS setup program (shown in [Figure 4-8](#)). In this example, you want to make sure that EPP is selected because it supports daisy-chaining.



**FIGURE 4-8:** Configuring the parallel port mode in CMOS.



**REMEMBER** *Daisy-chaining* is the feature of connecting one device off another, such as connecting the printer to the scanner and the scanner to the LPT (line print terminal) port.

The resources of the parallel port might also need to be configured if there are conflicts with another device. Notice that the default IRQ (interrupt request) for LPT1 is 7, and the default I/O address is 378-37F. You can read about IRQs and I/O addresses in Book 3, [Chapter 4](#). For now, just make a mental note that you can configure the IRQ and I/O address of the parallel port in CMOS.

## ***Serial ports***

A typical system includes two serial ports — COM1 and COM2 — and CMOS should have an entry for each of the serial ports. These entries enable you to change the resources, such as the IRQ and I/O address used by each of the serial ports, as shown in [Figure 4-9](#). The CMOS shown in [Figure 4-9](#) identifies the two serial ports as serial port A and serial port B. For more information on IRQs and I/O addresses, see Book 3, [Chapter 4](#).



**FIGURE 4-9:** Configuring the serial ports in CMOS.



**FOR THE  
EXAM**

Be sure to remember that the default IRQ for COM1 is 4, and the default IRQ for COM2 is 3. The default I/O address for COM1 is 3F8-3FF, and the default I/O address for COM2 is 2F8-2FF.

In the CMOS setup program, you can find not only an option to change the resources for the serial ports, but you can also disable the serial ports. Disabling the serial ports involves entering your CMOS program and switching a serial port to the disabled setting.

## ***Date and time***

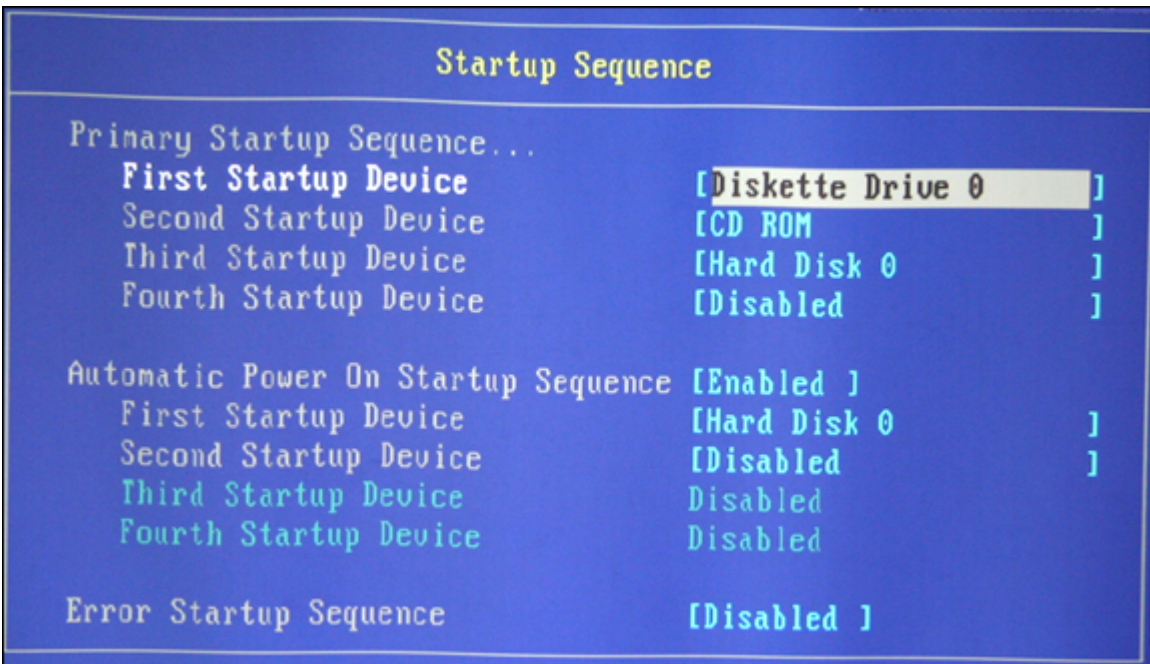
The date and time each have an entry in CMOS as well, which is where the operating system (OS) gets its date and time information. Setting the date and time in CMOS sets the date and time for the OS. From a troubleshooting point of view, you know that your CMOS battery is dying when during startup, the system asks you for the date and time. During startup after a battery failure, all the other settings are detected again — which is why you don't specify the hard disk or the floppy disk. However, the date and time must be specified again.

## ***Boot sequence/boot options***

Take special note of the CMOS entry for boot sequence or boot options; it determines what devices the system will try to boot from and in what order it tries each device. For example, older systems are typically set up to boot off a floppy disk first; if a bootable floppy disk isn't present, the system then boots off the hard drive.

Newer systems let you boot off a CD-ROM device or DVD, or even off the network first; and then, if no bootable device is found in either of those spots, proceed to boot off the hard drive. Booting off a CD-ROM or DVD device makes installing an OS extremely easy because most OSes today (like Windows or Linux) support booting off the installation CD to install the OS.

Most systems today are configured to try to boot from a floppy disk (if one exists), then a CD-ROM or DVD, then a hard disk, and finally a network. You determine the order to suit your needs, although typically, the floppy or CD-ROM drive is checked before the hard drive. If you like, you can disable devices, such as a CD-ROM drive, from being bootable. This is an important point because system security can be bypassed if a hacker can boot off his own CD containing his own copy of an OS. For security reasons, your company might consider disabling booting from floppy disk or CD-ROM. [Figure 4-10](#) shows the CMOS menu where you can configure the startup order for your system's devices.



**FIGURE 4-10:** Configuring the startup sequence in CMOS.

## ***BIOS security features***

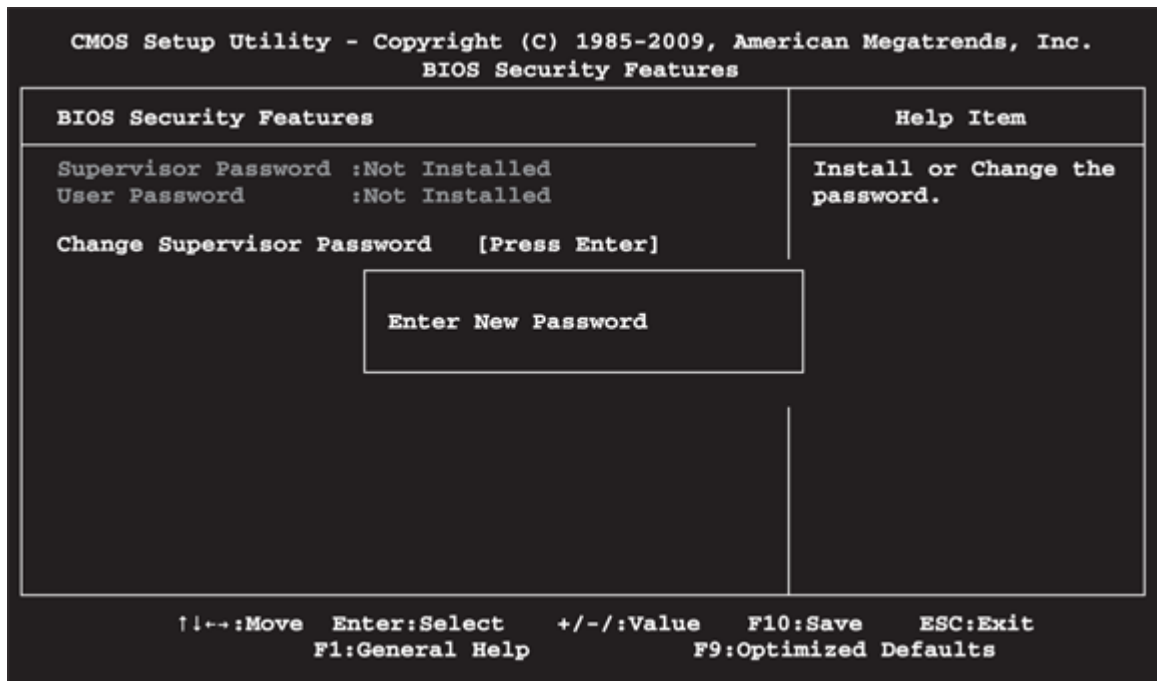
In this section, you learn about some of the security features found in CMOS, which is also known in the objectives as BIOS security. In the BIOS security settings, you can configure password settings, encryption settings, and intrusion-detection settings on some systems.

### ***User and administrator passwords***

In general, two types of passwords can be set in CMOS: the power-on password (also known as a *user password*) and the administrator password. The steps to set the password are different per manufacturer, but you will usually find the password option under a security or advanced menu in the CMOS setup program.

The *power-on password* is required to power on the computer. It is part of the power-on process and occurs before the OS is loaded. Many people like to call it a *hardware password* because the OS (the software) won't have a chance to load unless the correct password is entered. The implementation of power-on passwords can be especially useful in environments where security is a significant issue.

You set the *administrator password* in the CMOS setup program (shown in [Figure 4-11](#)). This password is required for anyone wanting to enter the CMOS setup program and make changes to the system configuration. It prevents unauthorized users from entering the CMOS setup program and changing the values that reside there.



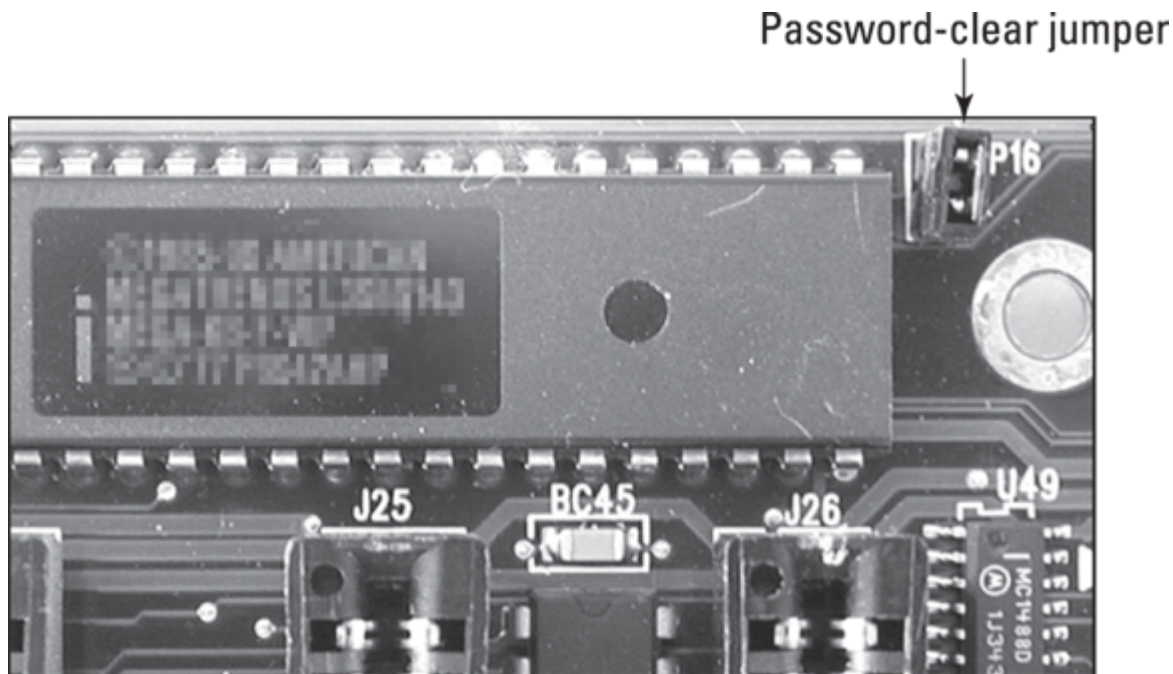
**FIGURE 4-11:** Setting an administrator password in CMOS.

When people get comfortable with computers, they start to explore the computer's options. Companies often end up spending time and money fixing problems that arise from the exploration of these options. This is why it might be useful to set an administrator password. The administrator password enables you to secure the workstation at the administrative level, and the power-on password allows you to secure the system at the user level — controlling who can use the system.

A question I often receive is, "What happens if you forget the CMOS password after it is set?" The answer is simple for desktops, but more difficult for laptops. First, check whether the motherboard has a jumper that can be removed to make CMOS forget the passwords (see [Figure 4-12](#)). After you remove the jumper to clear the password, put the jumper back on and power on the computer. Some systems have you place the



jumper over specific pins in order to clear the password; check the documentation to find out how to clear the password for your particular system.



**FIGURE 4-12:** A jumper that can be removed to erase the CMOS password.

If no such feature exists on your motherboard, you could remove the CMOS battery from the motherboard. Remember that CMOS RAM retains its information because there is a battery supplying power to the memory where CMOS data is stored. If you remove the battery, CMOS is erased, including the passwords (which is better than throwing away the system).

The only problem with removing the battery is that all the CMOS information is lost, including your hard drive, memory, and other device settings. The good news is that most of the information should be detected again on startup, such as the amount of memory installed or the size of the hard drive.



**WARNING** Earlier in this chapter, I mention that if your system asks you for the date and time when it boots up, this is usually an indication that

your CMOS battery is dead or dying. As noted here, the date and time aren't the only things lost to a dying battery. If security is an issue and your system keeps asking you for the date and time at boot-up, replace the battery *immediately* and then reset the administrator password to keep others, malicious or benign, from altering the CMOS setup.

A third solution to a forgotten password — and the one I like — is to get a CMOS utility, such as the CMOS Save & Restore utility. CMOS Save & Restore backs up the CMOS information and then allows you to restore it when an emergency arises. This solution involves backing up CMOS *before* a password is set so that CMOS can be restored to a state without a password. These utilities are popular ones that can be found on the Internet, and they back up the CMOS information to a text file. An example of a CMOS save and restore program can be found at

<http://mindprod.com/products1.html#CMOSSAVE>

### ***Support for drive encryption***

Drive encryption is a sought after feature today by companies that have employees carrying around company data on mobile devices such as laptops. With many systems today you can encrypt the entire drive, or volume, of the system. Without the encryption keys, an unauthorized person cannot

- » View the contents of the drive or volume.
- » Boot a system from the drive or volume.

The following common technologies help protect a company's data on a mobile device:

- » **TPM:** The *Trusted Platform Module* (TPM) is a chip on the motherboard that can be used with full drive or volume encryption to store the keys used to encrypt the entire drive. In order to use TPM encryption, you must have a TPM chip on the motherboard, and a TPM-enabled BIOS.



- » **Secure boot:** Secure boot is a feature of UEFI systems that adds a layer of security to the boot process. During the boot process, only authorized software (that is, software that has a valid signature) is allowed to run. This includes core boot code for the operating system. When the system boots, the firmware checks the signatures. If they are valid, the operating system is allowed to boot.
- » **LoJack:** Another BIOS security–related technology that is available to laptops is LoJack. LoJack, created by a company called Absolute Software, is a feature that allows the laptop to connect to Absolute Software’s servers to specify the laptop location and verify if the laptop was reported stolen. This feature allows companies and law enforcement to track the location of stolen property. The LoJack feature is disabled by default and can be enabled on the laptop after purchasing a license key from Absolute Software.

## *Plug and Play BIOS*

Most systems today have a Plug and Play BIOS (PnP BIOS). The term *plug and play* refers to the idea that you can connect a new device to the system, and the system automatically detects and configures the device to work with your system. To have a Plug and Play system, three conditions are necessary:

- » A Plug and Play device
- » A Plug and Play OS
- » A Plug and Play BIOS

If you are missing any one of these conditions, the OS cannot leverage Plug and Play and assign resources to a device on startup. On some older systems, you might see an entry in CMOS stating that it is a Plug and Play BIOS. All newer systems are Plug and Play BIOSes.

## *Viewing Advanced CMOS Settings*

Many newer systems maintain the basic CMOS parameters mentioned in the previous section but are also supplemented by different advanced setup settings. This section examines the purposes and characteristics of some of these advanced settings.

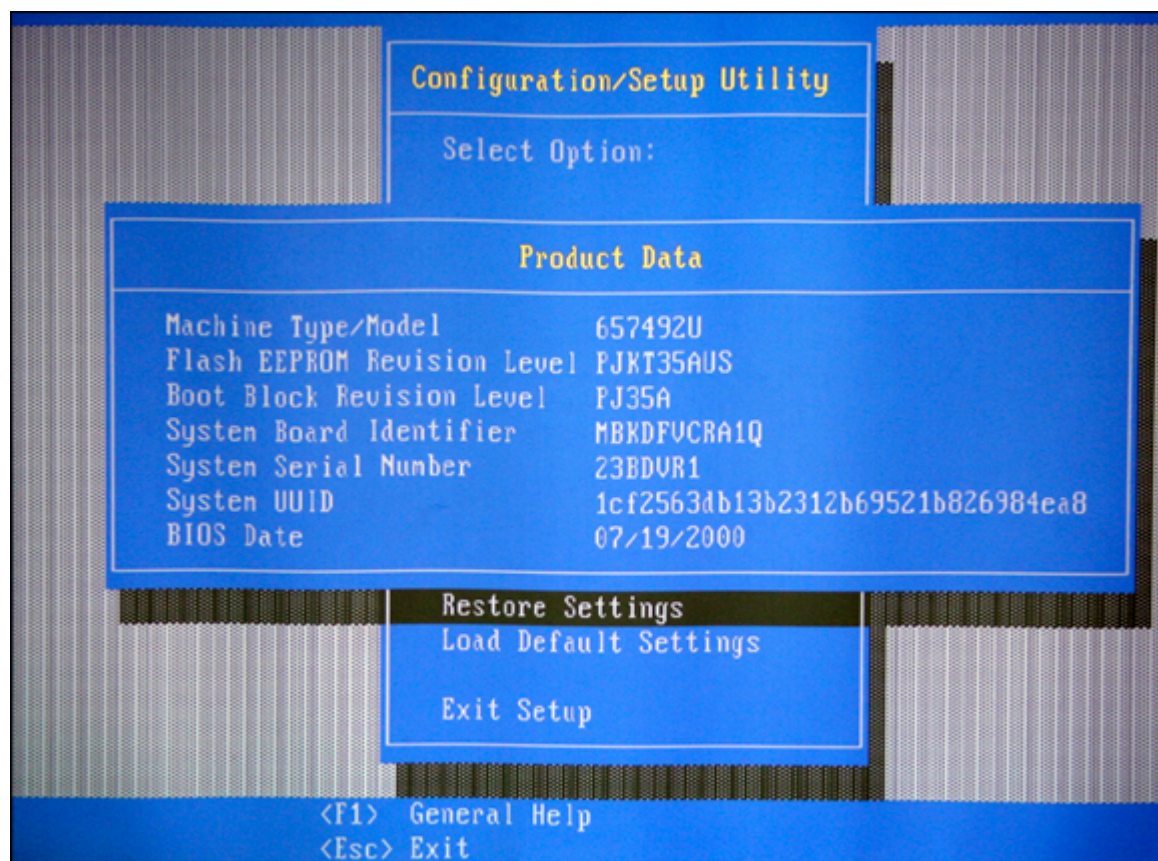
## *Globally unique identifier (GUID)*

The *globally unique identifier* (GUID) is a 128-bit number, randomly generated for the system when it was built, and stored in CMOS. The GUID uniquely identifies the system from any other. It enables the identification of individual computers and ensures that this identification method is absolutely unique.



**TIP**

Some systems have adopted the term *UUID* (universally unique identifier) instead of GUID. You might see a UUID in CMOS instead of a GUID, as shown in [Figure 4-13](#), but they are the same thing.



**FIGURE 4-13:** Viewing the system UUID and BIOS revision number through CMOS.

## ***BIOS date and revision number***

The date of your BIOS should be displayed somewhere in CMOS, usually under Summary Information. If you don't have a BIOS date, you might have a revision number or level. These entries in CMOS are important because you might be required to update your BIOS someday by going to the manufacturer's website and downloading the update. The first thing you will notice when doing this is that the manufacturer has built many different versions of BIOS for its systems. You need to make sure you get the proper update (the one for the date of your BIOS) by watching the revision number of your BIOS. For example, the site might instruct you to download BIOS update 1234 if you have Revision number R5.145. The big question is how to know what your revision number is. Check CMOS! Refer again to [Figure 4-13](#). You can see the BIOS version, or revision number, identified by the label Flash EEPROM Revision Level.



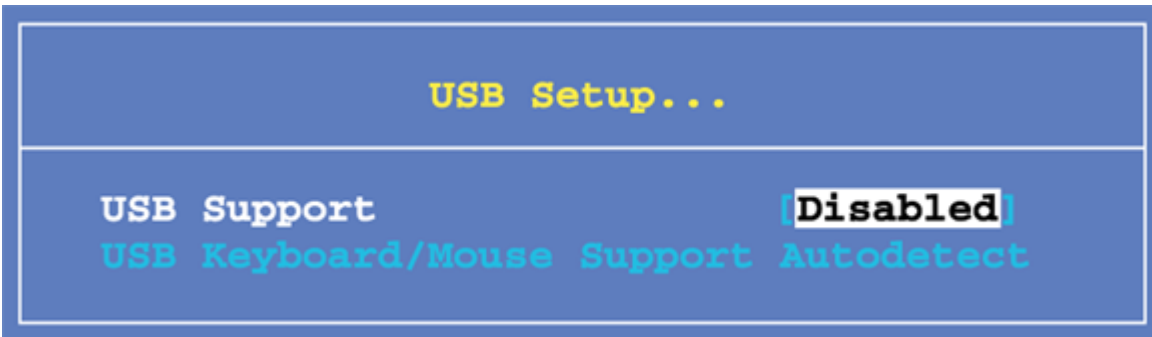
**TIP**

To ensure that you downloaded the correct BIOS update for the system, always make a note of the revision number and the date of the existing BIOS. Both pieces of information are typically used to determine which BIOS you need to download from the manufacturer's website.

## ***Universal Serial Bus (USB)***

Universal Serial Bus (USB) devices have gained much recognition over the last decade. USB devices are high-speed serial devices that use a single connector style and can be chained together with a *USB hub device*. A USB hub device connects all USB devices together at a central point. The USB hub may be its own unique device, or it may be just another device in the USB chain that has the capability of connecting other USB devices to it. For example, a USB monitor may have a USB port to allow a mouse to connect to it. Some popular USB-type devices include digital cameras, scanners, mice, and keyboards. You can even find USB network adapters.

If you have any problems getting a USB device connected to your computer, make sure the USB port has been enabled in CMOS. Also, remember that you can disable the USB ports in CMOS (as shown in [Figure 4-14](#)) to help secure your environment. You might want to do this to prevent a user on the network from using a flash drive to take home proprietary corporate data.



**FIGURE 4-14:** Disabling USB ports prevents using flash drives or other USB-type devices.

## *Built-in network adapter*

Most systems today come with built-in network interface cards (NICs) that allow the system to connect to a network or the Internet. Because the card is built-in, you do not have to buy a network card for the system. However, built-in network cards (or any built-in device) sometimes become faulty, but your system does not know that and always tries to use this built-in device anyway. Note that you can usually enable or disable the built-in network card through the CMOS setup program.

When your system includes a built-in network adapter, you usually have the option of enabling or disabling the capability to boot off the network as well. Unless this option is enabled, you cannot boot off the network, even if you specified a network boot in your startup order.



**FOR THE  
EXAM**

You need to verify three options in CMOS in order to boot off the network: that the network card is enabled, that your system has enabled booting off the network adapter, and then that the network

device is located in the startup order of devices. To boot off the network, you probably want the network as the first boot device.

In order to boot off the network, you need a *Preboot Execution Environment* (PXE)–compliant system. A PXE–compliant system is a system that has a BIOS that supports booting from a network card. For this to occur, you must ensure the network card is enabled and specified as a boot device within the CMOS setup. Once this is done, you can press F12 while the system is starting to boot off the network!

## ***Virus protection***

Some BIOS systems have built-in virus protection, which is (for the most part) a good thing. Some viruses attack the system by altering the *Master Boot Record* (MBR), which is the code that initiates the startup of the system and is located at the beginning of the hard drive. (For more information on MBR and hard drives, check out the next chapter in this minibook.) The virus protection built into the BIOS watches out solely for changes to the MBR and puts a stop to it!

Unfortunately, when you install a new OS, the installation modifies the MBR with its boot program files. As a result, the built-in virus detection in CMOS will see that “something” is modifying the MBR and will assume that it is a virus and stop the new OS from loading. In this case, you need to go into CMOS, disable the virus protection, and then restart the installation. After installation is complete, you will want to enable the virus protection in CMOS once again. [Figure 4-15](#) shows the startup options that indicate that virus protection has been disabled.





**FIGURE 4-15:** Viewing the virus protection setting in CMOS.

## *Onboard cache*

In Book 2, [Chapter 3](#), I discuss the benefits of cache and the types of cache memory, L1 and L2. In CMOS, you typically find an entry indicating how much cache memory exists on the system, and you can configure CMOS to disable this built-in cache memory.

Sometimes cache memory goes bad and causes boot-up problems. If having cache memory enabled presents any compatibility problems with your system, you can try disabling the cache memory as a troubleshooting technique. [Figure 4-16](#) shows the size of the cache memory and the option to enable or disable the cache memory. If the problem does not go away, there was no problem with the cache memory to begin with; enable the cache memory once again.

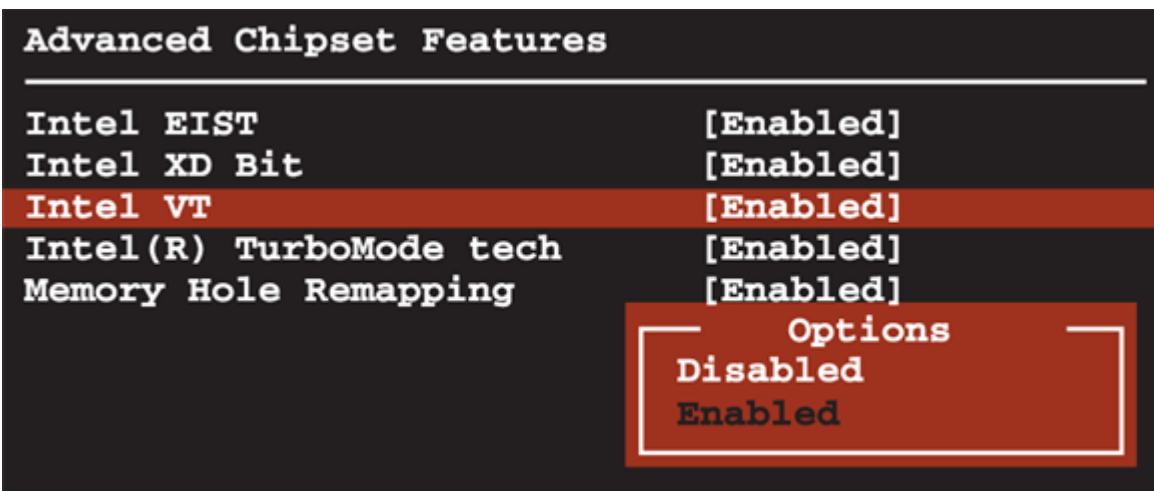


**FIGURE 4-16:** Disable built-in cache memory in CMOS to troubleshoot problems with corrupt cache memory.

## *Virtualization support*

Virtualization technology is one of the hottest technologies to come out over the last decade. Virtualization allows you to run multiple operating systems in their own *virtual machine* (VM), on the same physical computer. Each virtual machine is assigned resources such as memory, disk space, and processor. The benefit of virtualization is that a company can now run multiple systems as virtual systems on one physical machine. This results in less power consumption and makes better use of the asset the company has purchased.

In order to support today's virtualization technology, you must enable virtualization support in the system BIOS. This enables the firmware on the physical computer (known as the *host system*) that creates virtual machines, and is known as the *hypervisor*. [Figure 4-17](#) shows the display.



**FIGURE 4-17:** Enabling virtualization support in order to use VMs.

When looking to enable virtualization within the CMOS setup program, know that you are looking for one of two features. On Intel systems, you are looking for Intel Virtualization Technology (Intel VT) or AMD Virtualization (AMD-V) on AMD systems. Once you have located either of these settings, be sure to set the setting to enabled.



**TIP** If you are purchasing a system that will run multiple VMs, ensure the system has a virtualization-supported BIOS before making the purchase.

## ***Built-in diagnostics and monitoring***

Many systems today allow you to perform memory and/or hard drive diagnostics in order to identify problems with the systems that are due to memory issues or hard drive failure.

To perform the diagnostics, look for the diagnostics option in your CMOS and then choose the command to run the diagnostics. If there is a problem with memory or the hard drive, the system will report a diagnostics failure.

Some BIOSes today also have monitoring features that can monitor the health of the system. For example, you may have a monitoring option that reports to you the temperature of the system or maybe the speed at which the drives are turning. [Figure 4-18](#) shows the display.

```
System Diagnostics

F1      System Information
F2      Start-up Test
F3      Run-In Test
F4      Hard Disk Test

F11     Error Log
ESC     Exit

For more information, please visit:  www.hp.com/go/techcenter/startup
```



**FIGURE 4-18:** Performing memory diagnostics.

Some examples of monitoring features that may be supported by your BIOS are:

- » **Temperature monitoring:** The BIOS may report through the CMOS program the temperature of components such as the CPU.
- » **Fan speeds:** The monitoring features of the BIOS may report to you the speed at which the fans are running, which directly relates to the temperature of the CPU.
- » **Intrusion detection:** The intrusion detection monitoring will let you know if the computer case has been opened, keeping you aware of potential theft of components such as RAM or the hard disk from the computer.
- » **Voltage:** The monitoring features may report to you the voltage amounts being utilized by different components such as the CPU.
- » **Clock:** The clock speed may be reported indicating the speed of the CPU.
- » **Bus speed:** The monitoring feature may also report to you the speed of the different buses within the system.

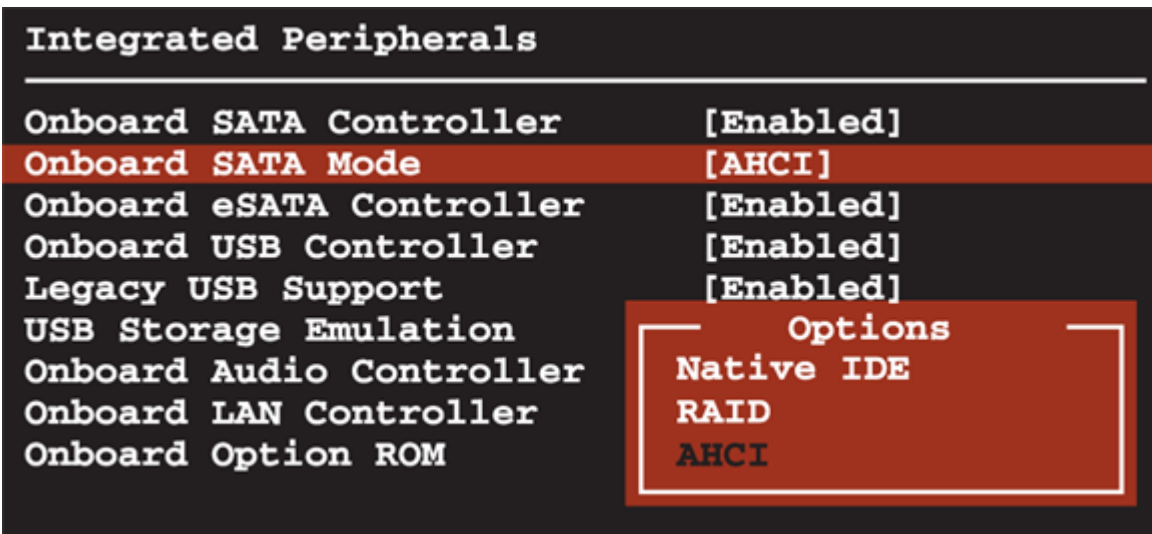
## ***AHCI settings***

The *Advanced Host Controller Interface* (AHCI) is a standard developed by Intel that allows software to communicate with SATA devices and take advantage of SATA features such as hot-swapping. Many system BIOSes today allow you to specify the operation mode of SATA through the AHCI mode in the BIOS settings.

With most systems today, you can configure the AHCI mode (see [Figure 4-19](#)) to any of the following:

- » **PATA Emulation:** Also known as *IDE compatibility mode* or *ACPI*, this mode emulates IDE and should be used if you are installing an older operating system, such as Windows XP, that does not have SATA drivers for your drive.

- » **AHCI Mode:** Enables SATA mode and should be used to gain the performance benefits of SATA if your operating system has a SATA driver. If the installation of the operating system does not detect the drive, try switching to IDE compatibility mode.
- » **RAID:** Used to support SATA in a RAID configuration.



**FIGURE 4-19:** Changing AHCI mode in CMOS.

## *Reserve resources*

If you are supporting older systems, you can reserve resources that have been assigned to legacy devices in CMOS. *Legacy devices* are non-Plug and Play devices, such as ISA (Industry Standard Architecture) cards, that have been added to the system. The ISA non-Plug and Play devices are hard-coded with a particular I/O address and IRQ, so you might need to configure CMOS to reserve the IRQ so that it is not given to a Plug and Play device on startup.

Removing the IRQ will ensure that a Plug and Play system will not assign the resources that are hard-coded into older devices to Plug and Play devices, which would create a conflict. Most systems today are Plug and Play, so unless you are supporting older hardware, you will most likely not hit this issue.



ON THE  
WEB

Now it is time to get some hands-on experience by performing Lab 4-1 and Lab 4-2. Lab 4-1 and Lab 4-2 can be downloaded from the companion website at [www.dummies.com/go/aplusaio](http://www.dummies.com/go/aplusaio).

## *Getting an A+*

In this chapter, you have learned about some of the common settings found in CMOS setup of systems today. You discovered the basic and advanced parameters in CMOS. The following points are covered:

- » The BIOS is low-level code used by the system to communicate with the system hardware. The BIOS code is stored on an EEPROM chip located on the motherboard of the system.
- » The BIOS is typically updated by downloading a BIOS update program and “flashing” the BIOS.
- » You enter a system’s CMOS setup program by using a keystroke such as F1 (IBM), F2 (Dell), or Delete when the system starts up.
- » You can change the boot order of the different bootable devices.
- » The three parallel port modes are SPP, EPP, and ECP.
- » You can change the hard drive from autodetect to manual so you can input the drive dimensions.
- » In order to support virtualization technology, you must have enabled virtualization support in the BIOS.
- » You can update your BIOS by downloading the BIOS update for your system from the BIOS manufacturer’s website.

## *Prep Test*

- 1. You have a USB camera from which you are trying to copy some of the pictures to the computer’s hard drive. The computer does not**

**seem to recognize the device. What should you do?**

- (A) Check to see that the boot order is correct.
- (B) Make sure that the USB ports are enabled.
- (C) Make sure that the serial port is enabled.
- (D) Make sure that the operating system has not assigned the USB device resources to some other device.

**2. You are part of the help desk support team for your company. One of your users calls complaining that the computer constantly prompts for the date and time. What does this indicate?**

- (A) The date and time are wrong.
- (B) The time has fallen back by one hour.
- (C) The battery on the motherboard is losing its charge.
- (D) The time has increased by one hour.

**3. You are installing Windows on a newer system with SATA drives, but the Windows setup program does not detect the drive. What should you do?**

- (A) Replace the BIOS with a non-Plug and Play BIOS.
- (B) Enable the AHCI IDE Compatibility option in CMOS.
- (C) Install an IDE drive.
- (D) Enable the AHCI RAID option in CMOS.

**4. Your manager is worried that someone will be able to start up any of the computers and view confidential information. What could you do to ensure that anyone starting the computer is supposed to be using that system?**

- (A) Lock the computer case.
- (B) Set file-share permissions on the files that are confidential.
- (C) Set a power-on password in CMOS.
- (D) Use NTFS permissions to protect the files from unauthorized access.

**5. You are installing Windows on your computer, and you know that the Windows CD is a bootable CD. You have tried a number of times to boot off the CD, but you are unable to. What CMOS option should you look for?**

- (A) You must delete the existing partitions so that you can boot off the CD-ROM.
- (B) Ensure that the CD-ROM device has been set up as the first device in the startup (boot-up) order.
- (C) Disable the hard drive in CMOS.
- (D) Disable the CD-ROM in CMOS.

**6. You are worried that some of your advanced computer users on the network will start changing the settings within CMOS. What is the best thing you can do to protect these settings?**

- (A) Set a power-on password.
- (B) Set an administrator password.
- (C) Set a Windows log-on password.
- (D) Ask the advanced users not to change any of the CMOS settings.

**7. Your built-in network adapter doesn't seem to be connecting you to the network. What is one of the first things you want to check for in CMOS?**

- (A) That the built-in network adapter is enabled in CMOS
- (B) That the network adapter driver is loaded
- (C) That the resources are not conflicting
- (D) That the proper protocol is installed

**8. You are trying to boot the system off the network, but the computer doesn't seem to boot off the network adapter. You have verified that the network adapter has been enabled in CMOS. What else should you check for within CMOS?**

- (A) That the network card has been disabled

- (B) That the network adapter has been disabled
- (C) That the CD-ROM has been configured as a bootable device
- (D) That the network adapter is set up as a bootable device

**9. You are experiencing a lot of problems running your customized software on some of the newer computers. What might you try disabling in CMOS to clear up the compatibility issue between the software and the system?**

- (A) RAM
- (B) Cache memory
- (C) Hard drive
- (D) Floppy drive

**10. You are having trouble installing a new operating system on your computer because the installation fails with each attempt. Which of the following CMOS settings would you disable to help the system make it through the installation?**

- (A) Network adapter
- (B) Bootable CD-ROM
- (C) Antivirus
- (D) Bootable network adapter

**11. Which of the following is a typical method for updating your system BIOS?**

- (A) Replace the old BIOS chip with a new BIOS chip.
- (B) Run a BIOS update program, also known as *firmware upgrade*, that flashes the BIOS with a new version of the BIOS.
- (C) Replace the old motherboard with a new one.
- (D) You cannot update the BIOS.

**12. Which of the following best describes the difference between BIOS and CMOS?**

- (A) BIOS contains the configuration information for the system, and CMOS is the low-level code that allows the devices to communicate.
- (B) BIOS is stored in RAM, and CMOS is stored in ROM.
- (C) BIOS is stored in RAM, and CMOS is stored in cache memory.
- (D) CMOS contains the configuration information for the system, and BIOS is the low-level code that allows the devices to communicate.

## Answers

1. **B.** In today's systems, many of the built-in devices can be enabled or disabled in the CMOS setup program. When experiencing problems with a built-in device, the first thing you should check is whether the device is enabled. See "[\*Built-in network adapter.\*](#)"
2. **C.** The CMOS configuration information is stored in CMOS RAM. This special RAM chip maintains its information by using a small battery on the system board. If the battery loses its charge, the CMOS RAM is flushed out, meaning that it will prompt you for the information such as the date and time as the system boots up. Review "[\*Date and time.\*](#)"
3. **B.** The newer CMOS setup programs allow you to change the configuration so that the SATA is emulating an IDE interface. This can allow software that is not SATA aware to recognize the drive. Check out "[\*AHCI settings.\*](#)"
4. **C.** Choice C is the best answer to ensure that only authorized individuals are powering on the system. In order to use the system, someone will need to type the CMOS password. This password is not dependent upon any particular operating system because you are setting a hardware-level password. Peruse "[\*User and administrator passwords.\*](#)"
5. **B.** Many computers are set up to boot off the floppy drive, then the hard drive, and finally the CD-ROM, which means that if the system can boot off the floppy or hard drive, the opportunity will never arise to boot off the CD-ROM. Changing the startup order so that the CD-

ROM is the first bootable device means that you can put in the Windows CD-ROM, and setup will be invoked from it. Choice A would work, assuming that the CD-ROM device is listed anywhere in the bootable device order. Unfortunately, you have lost the contents of the hard drive because partitions have been wiped out, so Choice A is not the best answer. *Take a look at “[Boot sequence](#).”*

6. **B.** An administrator password is a password that must be provided to enter the CMOS setup program and change the settings. Choice A is not the right answer because you might not want to set up a password for when the computer turns on but only if a user tries to enter the CMOS setup program. *Peek at “[User and administrator passwords](#).”*
7. **A.** One of the first things you want to do with a built-in device is ensure that the device has not been disabled in CMOS. If it has not been disabled, you should look at the other choices for the solution. *Study “[Built-in network adapter](#).”*
8. **D.** When booting the system from the network, you need to ensure that the computer not only has the network adapter enabled, but also that the network adapter is signified as a bootable device, and maybe even the first bootable device. In this question, you have already verified that the network adapter has been enabled, so Choice D is the only possible answer. *Refer to “[Built-in network adapter](#).”*
9. **B.** Many systems today have built-in cache memory. Although it isn't that common, you might sometimes have problems with particular software not “liking the idea” of using information from cache instead of RAM. To test this, temporarily disable the cache memory. *Examine “[Onboard cache](#).”*
10. **C.** Viruses commonly attack the MBR of the hard drive, so virus software constantly watches out for applications that try to make a change to this area of the disk. Some systems today have built-in virus detection, and because the installation of a new operating system causes a change to the MBR, there may be incompatibilities between the OS installation and the virus protection built into the system. Disabling this virus protection in the CMOS will allow the installation to finish. *See “[Virus protection](#).”*



11. **B.** To update your BIOS today, you will download the update from the Internet and then run the update. In the past, you would have to replace the entire ROM chip. *Review “Performing BIOS upgrades/firmware updates.”*
12. **D.** CMOS is the inventory list of devices and their configuration, whereas the BIOS is the set of low-level instructions that tells these devices how to communicate. Choice B and Choice C are wrong because BIOS code is stored in ROM, not RAM. *Check out “[BIOS versus CMOS](#).”*

# Chapter 5

## Working with Storage

---

### IN THIS CHAPTER

- » Understanding hard drive terminology
  - » Discovering IDE devices
  - » Learning how SCSI works
  - » Mastering SATA disks
  - » Using removable storage
- 

One of the primary responsibilities of a PC technician is managing hard disks. This responsibility involves more than just partitioning and formatting disks; it also entails installing disks into the computer system and configuring the system to recognize the newly added disks.

In this chapter, you discover the skills that you need for installing, configuring, and troubleshooting hard disks. I introduce you to a new world of terminology related to hard disk installation and configuration, along with other types of storage like CD-ROMs and DVDs.

In this chapter, I also make sure you understand the difference between IDE, SCSI, and serial ATA (SATA) devices. You also see the steps required to install and configure IDE master/slave devices in a chain and the steps required to install a SCSI bus.

## *Understanding Hard Drive Terminology*

If you took a martial arts class, the instructor would show you how to do some basic punches and kicks before letting you spar or compete. The instructor would be well aware that jumping into combat without the

basics could do you more damage than good. PC repair works the same way: Before discussing the installation and configuration of IDE and SCSI devices, it is important to cover some basic terminology surrounding hard drives.

Hard drives are used to store data so that the data can be retrieved at a later time. A hard drive can be internal to the system using technologies such as IDE, SCSI, or SATA (you find out more about those technologies as the chapter progresses), or the drive can be an external drive connected via USB, FireWire, or eSATA.

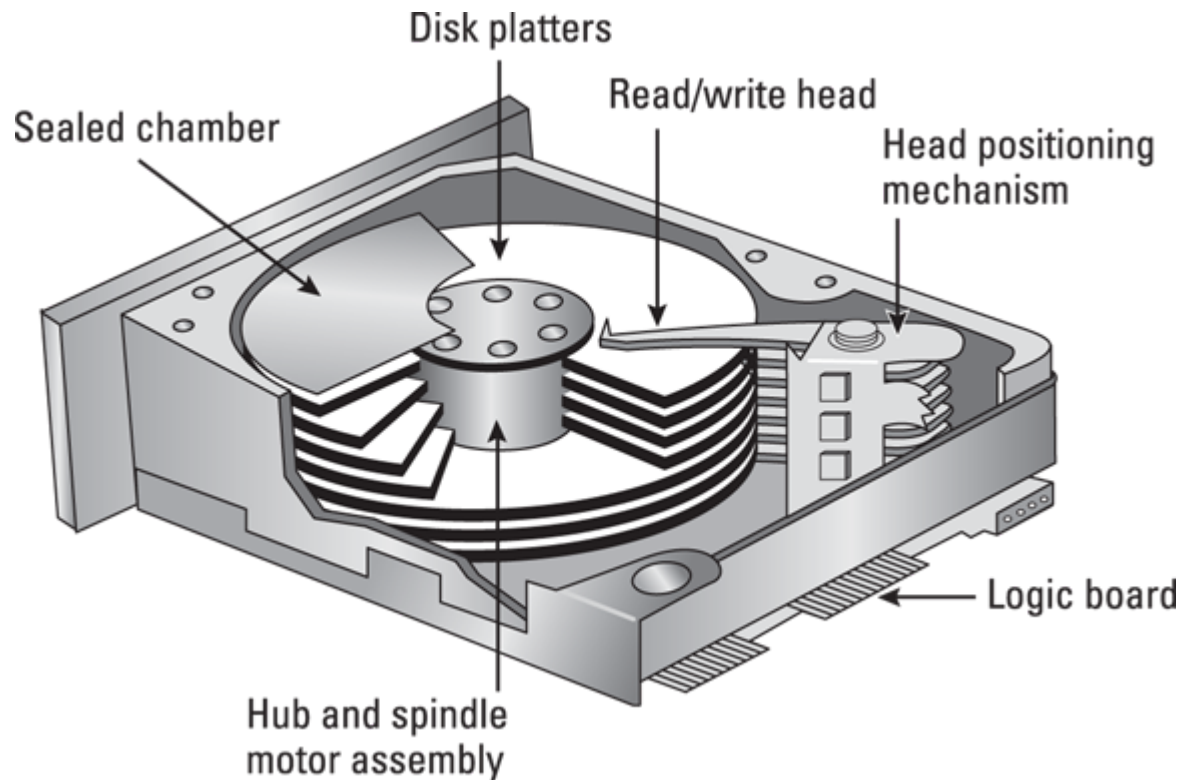
You can also purchase *network attached storage (NAS)* today that connects to the network via an Ethernet connection. What is also exciting about today's systems is that the drives are hot swappable, meaning that you can disconnect and connect the drive with the system running.

## ***Disk geometry***

The following sections introduce you to *disk geometry* — essentially the physical components of a drive that make up your data storage solution. You also find out some general terminology about hard drives and hard drive storage in this section.

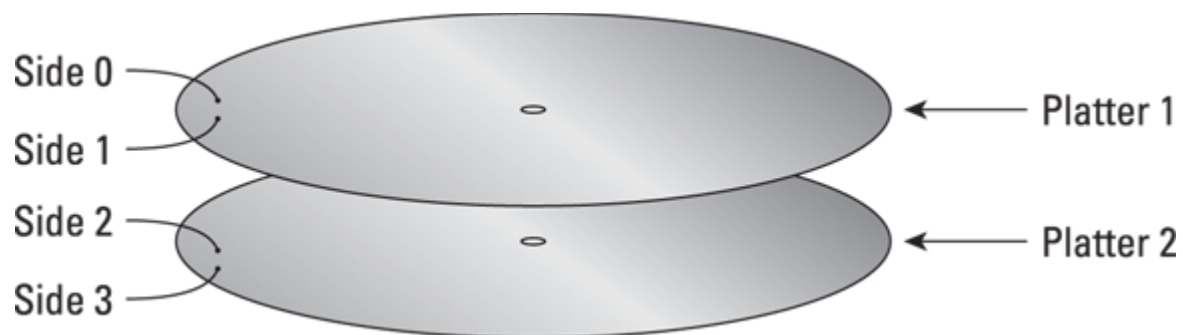
### ***Platters***

A *platter* is a physical object (actually, a plate) inside the hard disk that is responsible for storing the data. A platter is similar to a music record (remember those old LPs your parents or grandparents had around the house?) in the sense that it spins on a spindle that runs through the center of the platter. A hard disk has many platters. [Figure 5-1](#) shows the platters inside a hard disk.



**FIGURE 5-1:** The internals of a hard disk.

Not only are the platters similar to records on a record player in the sense that they spin on a spindle that runs through the center of all the platters, but they also store the data on tracks like tracks on a record. Each platter has two sides for storing information, and each side of the platter has a unique ID. The ID for the first side of the first platter is 0, and each side increases by 1. For example, two platters are in the disk, the first platter has side 0 and side 1, and the second platter has side 2 and side 3. [Figure 5-2](#) illustrates this concept.



**FIGURE 5-2:** Sides of a platter.

Because each side of the platter has a writing mechanism, many people use the terms “head” and “side” interchangeably. The head is more accurately called the *read/write head* because it moves over the disk surface and reads from or writes to the disk. Like a needle on a record player, the read/write head moves over the surface of the disk with the help of an arm, called the *actuator arm* or the *head positioning mechanism*. [Figure 5-1](#) illustrates the read/write head on an actuator arm.



**TIP** Each platter surface on the disk has its own read/write head. When information is written to the disk, the read/write head moves to the same track on all platters in a single movement and then writes the data across the same track on all platters. The actuator arm has multiple read/write heads on it.

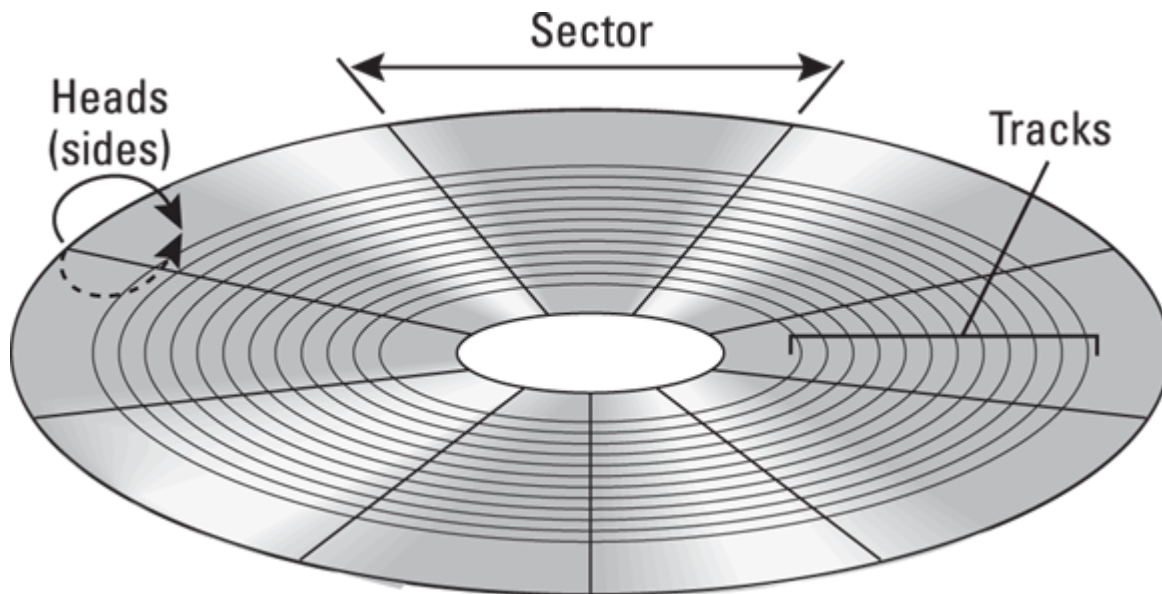
## ***Tracks***

Just like there are grooves (tracks) on a music record, there are also *tracks* on each platter. These tracks are evenly spaced across the platter’s surface.

## ***Sectors***

The platter is divided into pie-shaped slices, called *sectors*. Now the confusing thing about sectors is that where a track intersects with a sector, *sector blocks* are created — also known as sectors! Each sector (block) — 512 bytes in size — is the actual storage area for data. Under the hood, the drive controller may not actually use 512 bytes, but use a larger value and emulate 512 bytes for backward compatibility.

[Figure 5-3](#) illustrates the tracks and sectors on a disk platter. Each pie-sliced sector has an address; the first sector is sector 1, the second sector is sector 2, and so on. The reason why the term sector applies to two different areas of the disk is because if you were to look at a sector (the pie slice), like the pie slice labeled in [Figure 5-3](#) as “Sector,” it might be sector 1. All sector blocks in that pie slice are considered sector 1 as well, but they differ in the track that they reside on.



**FIGURE 5-3:** Tracks and sectors on a disk platter.

So, each sector block has an address comprising the platter side number, the sector, and track number. For example, data can be saved to side 1, sector 2, track 4 — which is the address of a 512-byte sector block. Note that the term *sector block* is a term I made up for this discussion; the term *sector* is also used to describe the 512-byte blocks.

### Clusters

A group of sectors makes up a *cluster*, which is the allocation unit for a file — meaning where a file is saved. When a *partition* (a logical division of space on the disk) is formatted, the file system determines the cluster size based upon the partition size. For example, a 2GB FAT partition uses a 32K cluster size. That same 2GB partition formatted as FAT32 uses only a 4K cluster size.

Having a partition use a 4K cluster size means that eight sectors make up a cluster. Keep in mind that after a file is saved to the cluster, no other file can occupy that cluster. For example, if you have a 32K cluster size and you save a 3K file to the hard disk, the file is saved to an empty cluster — but only 3K of that cluster is used, and the remaining 29K is empty. The remaining 29K is now considered unusable space; no other file can be saved to that unused 29K.

### Cylinders

All platters in the hard disk contain the same number of tracks, but that number varies from one hard disk to another. These tracks are numbered from the outside in, starting with 0 (zero). For example, on a platter with ten tracks, the track closest to the outer edge of the platter is track 0, and the track closest to the center is track 9.

A *cylinder* consists of the same track on both sides of all the platters. In other words, when you reference track 0, you reference a particular track on a particular platter; however, when you reference cylinder 0, you reference track 0 on all platters.

If you know the number of cylinders, heads, and sectors per track, you can calculate the size of a disk. For example, if a drive has 4,092 cylinders, 16 heads, and 63 sectors per track, the size of the disk is 2,111,864,832 bytes (2.1GB). The formula to calculate the size of the disk is

$$\begin{array}{l} \text{cylinders} \times \text{number of heads} \times \text{number of sectors per track} \times 512 \\ \text{bytes per sector} \end{array}$$

## ***Read/write process***

Platters are typically divided into 512-byte sectors. These sectors are the area on the platter that data is written to. The platters have a magnetic coating applied that is extremely sensitive to magnetism. While the platters spin, the read/write head moves from track to track until it reaches the desired track. Then it waits for the appropriate sector to move underneath it, at which time the read/write head is energized to apply a magnetic charge to the particles in the disk coating. This changes the particle binary state from 0 to 1, thus creating data. The same happens when the data needs to be read: The read/write head moves over the appropriate sector and reads the data that resides in the sector.

The read/write heads don't actually touch the surface of the disk platters; instead, they hover about 10 micro-inches (or millionths of an inch) above it. (That's not even enough space to place a hair between the read/write head and the platter's surface.) This design helps improve disk performance because a read/write head that makes contact with the platter

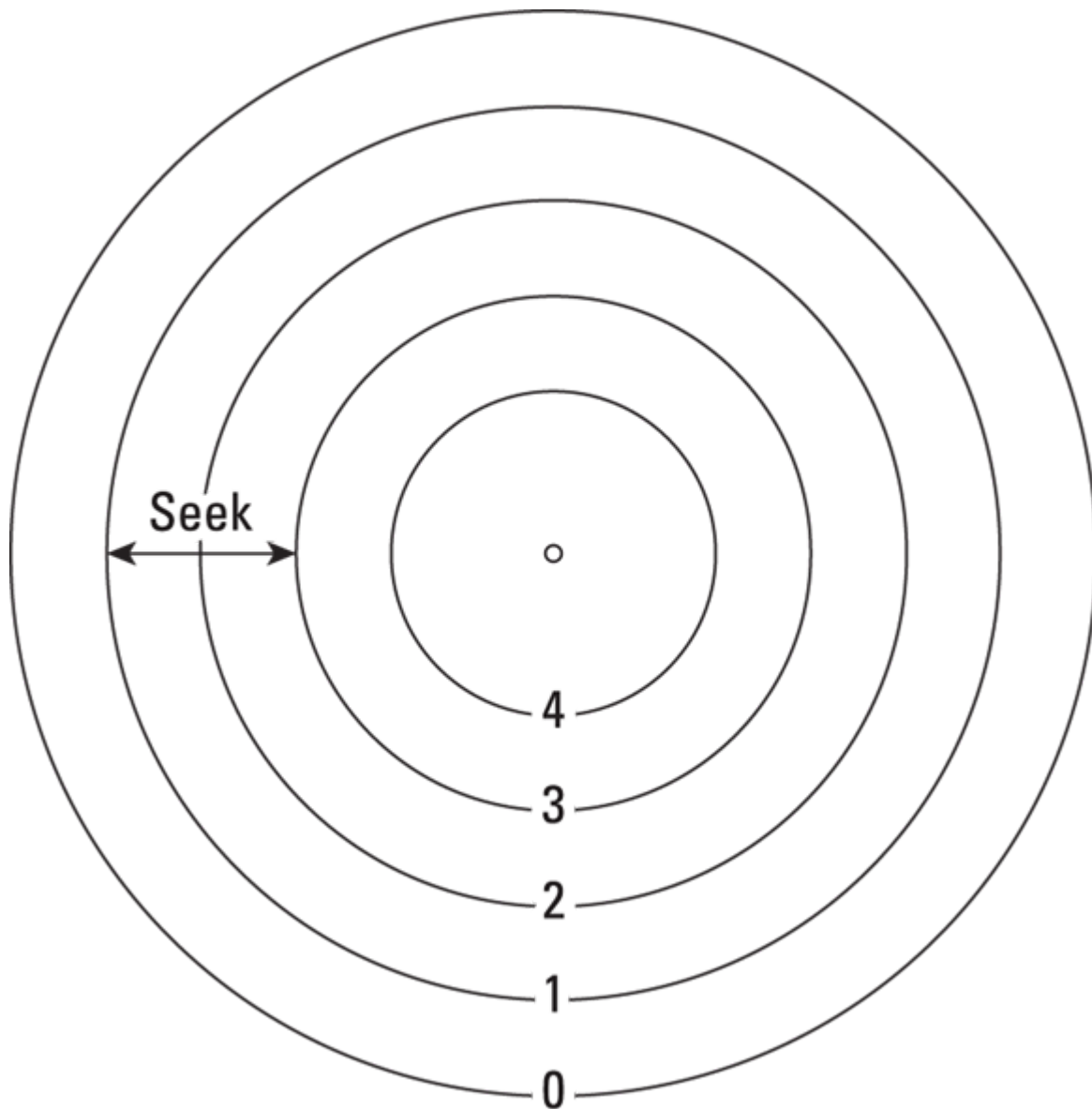
causes friction, slowing down the rotation speed of the disk and creating extra heat.

## *Performance*

Magnetic disk performance can be measured in terms of several important characteristics:

- » **Seek time** is how long it takes to move the read/write heads to the desired track. Seek time is a calculated average because the time it takes to move to the desired track differs from one instance to another. For example, if the read/write heads are on track 1, they will take longer to move to track 12 than to track 3. Seek time is measured in milliseconds (ms), or one-thousandth of a second. [Figure 5-4](#) shows how seek time is measured.
- » **Latency** is how long it takes for the appropriate sector to move under the read/write head. Latency is measured in milliseconds.
- » **Access time** describes the overall speed of the disk. It is a combination of seek time and latency. The lower the access time, the better.
- » **Spin speed** is how fast the platters spin, measured in rotations per minute (rpm). The larger the rpm value, the faster the disk, which means less latency.





**FIGURE 5-4:** Measuring seek time.

I want to make a note about the spin speed of the drive. Today, the rpms are how we measure the speed of the drive. Common examples of rpms are 5,400 rpms, 7,200 rpms, 10,000 rpms, and finally 15,000 rpms. The more rotations per minute (rpm), the faster the drive is. For example, a 7200-rpm drive is faster than a 5400-rpm drive. A typical drive you install today in a workstation is 7200 rpm. You may want to install faster drives in servers.

### ***Master Boot Record***

The *Master Boot Record (MBR)* is the first sector on the first track of the first side of the first platter; it holds the operating system (OS) boot code that controls the loading of the OS.

The MBR also holds drive characteristics, such as the partition table. During the boot process, the system has to find a primary partition that is active — it does this by looking at the partition table in the MBR.

In general, if anything goes wrong with the MBR, you will not be able to boot the system. Because the boot record is always in the same location on every disk, it becomes very easy for a malicious hacker to write viruses that modify or corrupt the MBR. This is one reason you should always run virus-detection software. See Book 9, [Chapter 3](#) for more on virus detection and protection.

## *Troubleshooting MBR disks*

CompTIA wants you to know some common command-line tools for troubleshooting hard disks. Technically, these tips and tools apply to either MBR or GPT disks, but it makes sense to me to include them here. When troubleshooting a Windows 10 system, you can gain access to these tools on a Windows 10 system by restarting the computer into the Windows Recovery Environment (RE).

- » **BOOTREC** is a “Swiss Army Knife” utility that can repair all sorts of MBR problems. Specifically, remember the `/FixMbr`, `/FixBoot`, `/ScanOS`, and `/RebuildBCD` parameters for your A+ exams.
- » **CHKDSK** is an ancient file system scanning and repair tool.
- » **FORMAT** is used to prepare a hard disk partition by laying down a file system and assigning a drive letter; at that point the partition becomes a volume.
- » **DISKPART** is the command-line equivalent to the Disk Management MMC console in Windows.
- » **DEFRAG** is the command-line variant to the Windows 10 Disk Defragmenter tool. Running this command periodically on magnetic disks will maximize disk I/O performance.

- » **File recovery software** varies in Windows, depending on the operating system version. Windows 10 includes the File History feature, which saves copies of your work periodically to another volume and can restore previous copies of content that you've changed or deleted.

## *Discovering IDE Devices*

In the following sections, you find out how to install and troubleshoot IDE devices. First, you get an overview of IDE devices and some of their features, and then you see a number of different configurations for installing IDE devices into a computer system.

Before your operating system, be it Windows, macOS, or Linux, can work with any type of hard drive, you must initialize the disk by using the appropriate OS feature or tool. For example, use the Disk Management utility to initialize IDE, SATA, and/or USB disks. Having said that, let's continue our detailed consideration of the historically relevant IDE hard disk drives.

### *IDE overview*

The *hard drive controller* is responsible for converting signals made by the system CPU to signals that the hard disk can understand. These signals include instructions on where to find data and how to get to that data. The hard disk performs its task, and any data that needs to be returned is sent to the controller from the hard disk. The controller then converts the signals from the hard disk into signals that the system can understand.

In the past, the controller was on an expansion card, which was connected to the drives via ribbon cables. The goal of IDE was to make the installation of hard disks easier by including the controller on the hard disk, which is where the name comes from: *Integrated Drive Electronics* (IDE). So, today's drives have the controllers integrated into the drives themselves, meaning the drive is its own boss.

Originally, IDE was available only in the flavor of hard drives; you did not have any other type of IDE device, such as CD-ROM or tape drives.

IDE hard drives had a maximum capacity of about 528MB. Another important limitation with IDE is that only two devices could be connected in a chain. Back in the day when IDE was first used, SCSI was better in that respect because it supported eight devices in a chain. (Read more on SCSI in the later section, “[Learning How SCSI Works](#).”)

Original IDE devices have a transfer rate of about 10 MBps and may have cache on the drive itself. *Cache memory* is a small amount of memory for storing data frequently used to increase drive performance.

Because of its limitations, IDE has been replaced by *Enhanced Integrated Drive Electronics (EIDE)*. EIDE devices have a transfer rate of about 16 MBps. Four devices are allowed in an EIDE chain, with a greater variety available. For example, you may now add CD-ROMs and even Zip drives to an EIDE chain. Note that the capacity of the drives has been dramatically increased with EIDE — it now supports drives of over 200GB! [Table 5-1](#) compares the features of IDE and EIDE.

**[TABLE 5-1](#) IDE versus EIDE**

<i>Characteristic</i>	<i>IDE</i>	<i>EIDE</i>
Size	528MB	200GB and higher
Devices in chain	2	4
Transfer rate	10 MBps	16 MBps and higher
Types of devices	Hard drives	Hard drives, CD-ROMs

IDE has been around for quite some time now and has gone through some changes. The following sections outline some technologies and terms that describe the different versions of IDE. Be sure to know these for the A+ exams.

### ***IDE/ATA standard***

A number of hard drive standards have been developed over the last two decades, the first major standard being the IDE standard. The IDE standard, which has been around since 1989, calls for an integrated controller on the drive to manage information entering and leaving the hard disk.

IDE drives attach to the motherboard by means of a 40-wire ribbon cable. The IDE standard also allows two drives to daisy chain, creating a master/slave relationship between devices. The master drive is responsible for sending and receiving information in the chain.

The IDE standard is also known as the Advanced Technology Attachment (ATA) standard, sometimes called the ATA-1 standard.

### ***EIDE/ATA-2 standard***

The EIDE standard followed shortly after the IDE standard. The EIDE standard allows four drives to be connected to a dual-channel controller. This is usually implemented as a motherboard with two connectors (also known as controllers) — one primary and one secondary. You could then connect two drives off of each controller, making a master/slave chain for each controller. EIDE also supports larger hard disks than the original IDE standard; the original size of an IDE drive was approximately 528MB. The EIDE standard is also known as ATA-2 standard.



**TIP**

Most techies in the computing industry interchange *IDE* and *EIDE*. For example, if you have a newer motherboard that uses EIDE drives, most documentation and technicians simply use the term *IDE* even though the drives might be EIDE, or even an Ultra DMA (direct memory access) drive. Also note that most techies and documentation use the term “controller” for the connectors on the motherboard that you connect the drives to, but really the controller is the circuitry on the hard drive that controls access to the drive. My point is get used to people using the term *IDE* instead of *EIDE*, and *controller* instead of *connectors*.

### ***ATAPI specification***

Originally, IDE devices were implemented as hard drives, but an additional ATA specification allows other types of devices to exist on an ATA (or IDE) chain. This specification is the ATA Packet Interface (ATAPI), which allows devices like CD-ROMs and tape drives to exist

on an ATA chain. Other types of ATAPI devices are legacy CD/DVD devices.

### *Drive performance*

The performance of the drive is determined by the Programmed I/O (PIO) mode or DMA mode it supports. The PIO mode or DMA mode is a protocol that determines the transfer rate of the drive. A number of different PIO modes and DMA modes are supported by devices, as shown in [Table 5-2](#).

**TABLE 5-2** PIO and DMA Modes

<i>Mode</i>	<i>Runs At</i>	<i>Used By</i>
PIO Mode 0	3.3 MBps	ATA-1
PIO Mode 1	5.2 MBps	ATA-1
PIO Mode 2	8.3 MBps	ATA-1
PIO Mode 3	11.1 MBps	ATA-1 and ATA-2
PIO Mode 4	16.6 MBps	ATA-1 and ATA-2
DMA 33	33.3 MBps	Ultra DMA drives
DMA 66	66 MBps	Ultra DMA drives
DMA 100	100 MBps	Ultra DMA drives
DMA 133	133 MBps	Ultra DMA drives



**FOR THE  
EXAM**

Be sure to know what a PIO mode is and also the transfer rates of Ultra DMA drives.

### *Installing IDE devices*

In this section, I show you how to install an IDE device. Because all hard drives are different, I present only the most popular solutions for installing hard drives.

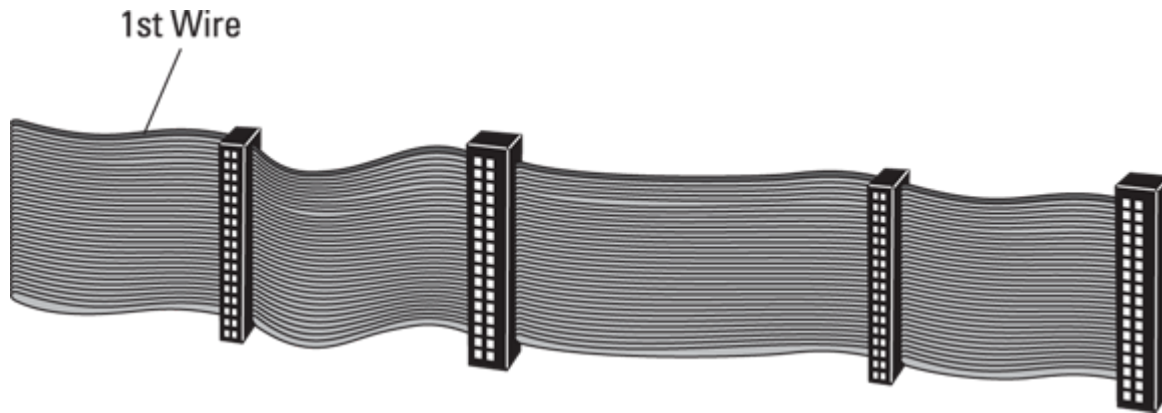
First, you want to open the casing of the computer and find an empty bay for mounting the new hard disk. If you are removing the old hard drive, you can use the same bay. If you are adding a hard drive, find an empty bay and mount the drive there. Second, you slide the drive in the bay so that the power connector and ribbon cable connector face the motherboard. [Figure 5-5](#) shows an IDE drive being placed into the mounting bay.



**FIGURE 5-5:** Mounting the hard disk into the drive bay.

### *IDE cabling*

After you mount the drive into place, the third step is to connect the IDE connector on the motherboard to the IDE connector on the hard disk with a 40-wire IDE ribbon cable. Then connect a power connector to the drive. [Figure 5-6](#) shows an IDE ribbon cable.



**FIGURE 5-6:** An IDE ribbon cable.

One of the wires (wire 1) on the IDE ribbon cable is a different color than the others; usually, it's red, but it might be blue. Wire 1 must be placed over pin 1 when connecting the ribbon cable to the hard drive and motherboard — the Pin 1 rule.

The big question is how to determine which pin is pin 1. Hopefully, the manufacturer indicates pin 1 by placing a small 1 near it. If you look at the connector on the hard drive and on the motherboard, you might see a small 1 on one end of the connector. That's where you need to place wire 1 when connecting the ribbon cable.

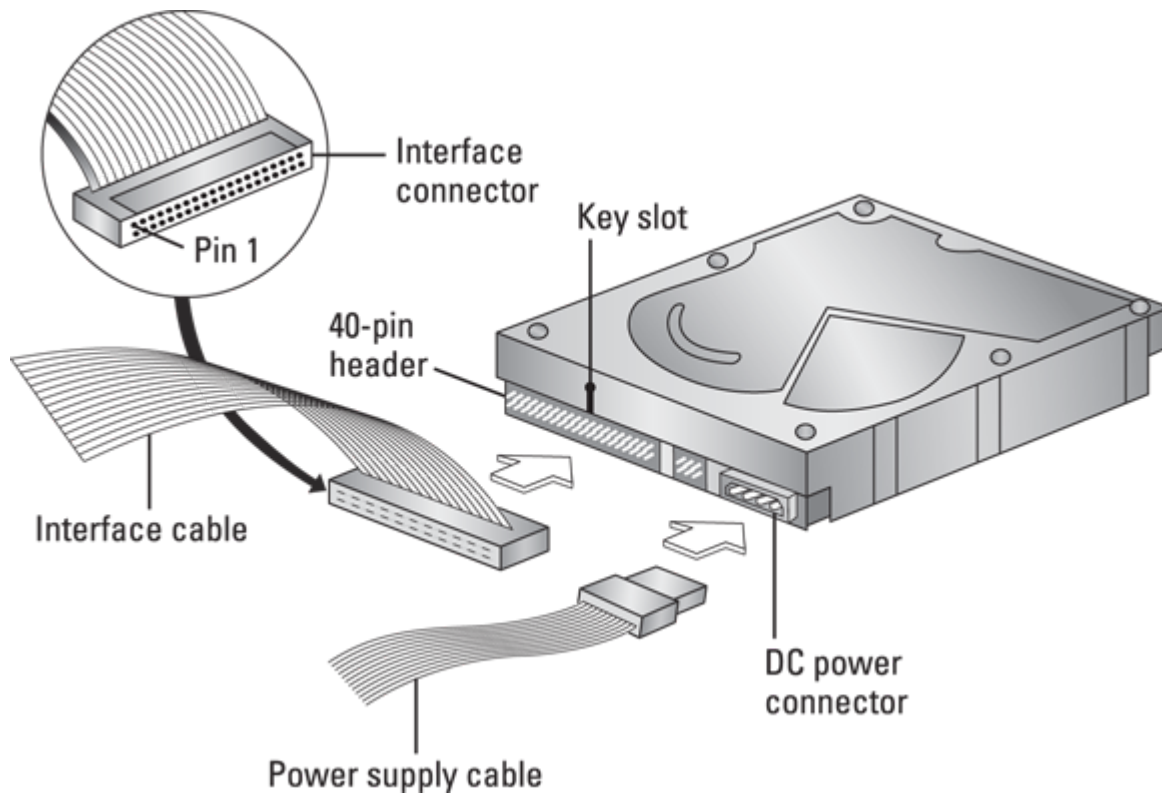


**TIP**

Sometimes a manufacturer might not have enough space to indicate pin 1 and so does the opposite — indicate pin 40. This method gives you the same information, though: If you know what side pin 40 is on, you know that pin 1 is on the opposite side.

After you connect the IDE ribbon cable, connect the hard disk power from the power supply so that you can run the motor in the drive. (People often forget this step and then wonder why the drive doesn't work.) [Figure 5-7](#) shows how to connect the ribbon cable and the power supply cable to the hard disk.





**FIGURE 5-7:** Connecting an IDE drive.

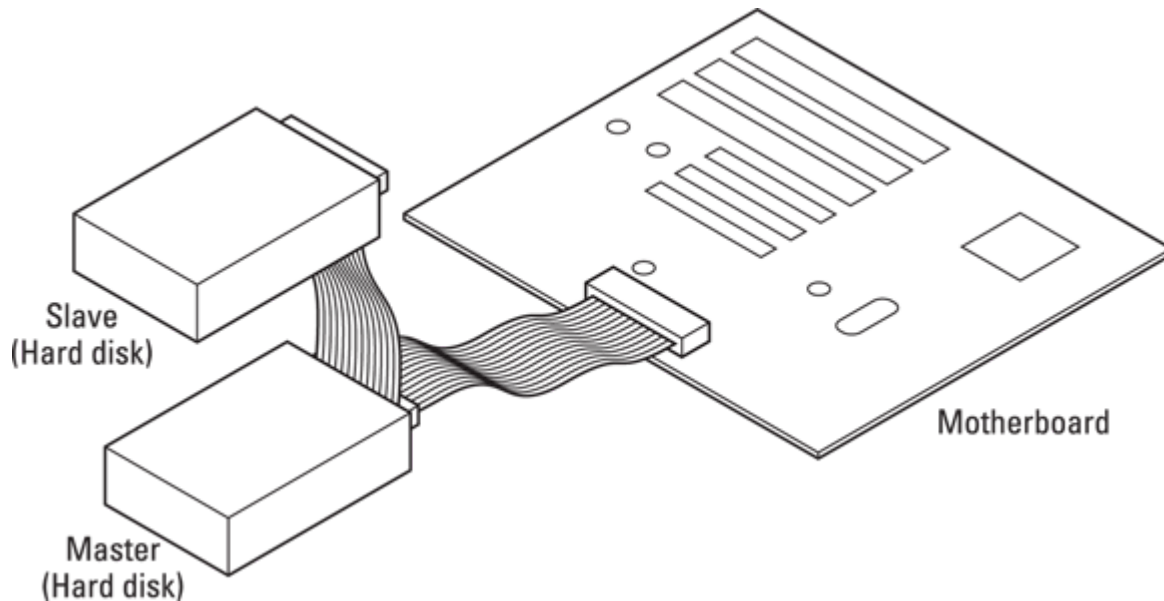
### ***Master/slave configuration***

If you are installing multiple IDE devices, you are creating an IDE chain. The chain will be made up of one 40-wire IDE ribbon cable with two drives connected to it. Most IDE ribbon cables today have three IDE connectors on them: one that connects to the motherboard and one for each of the two drives that can be connected in a single chain.

After the two drives are connected, configure the drives into a master/slave configuration. Use this type of configuration because each drive has a built-in controller that makes it act like its own boss. (Have you ever tried to work in an environment with two bosses? Not good.) The purpose of designating a master is to specify the boss of that chain — the controller responsible for communicating with the processor.

When setting up a multidrive system, you have two drives, each with a controller that can potentially send signals to and receive from the processor. To save confusion, one of the drives is designated as the *master*, which receives all signals from the processor and sends back any

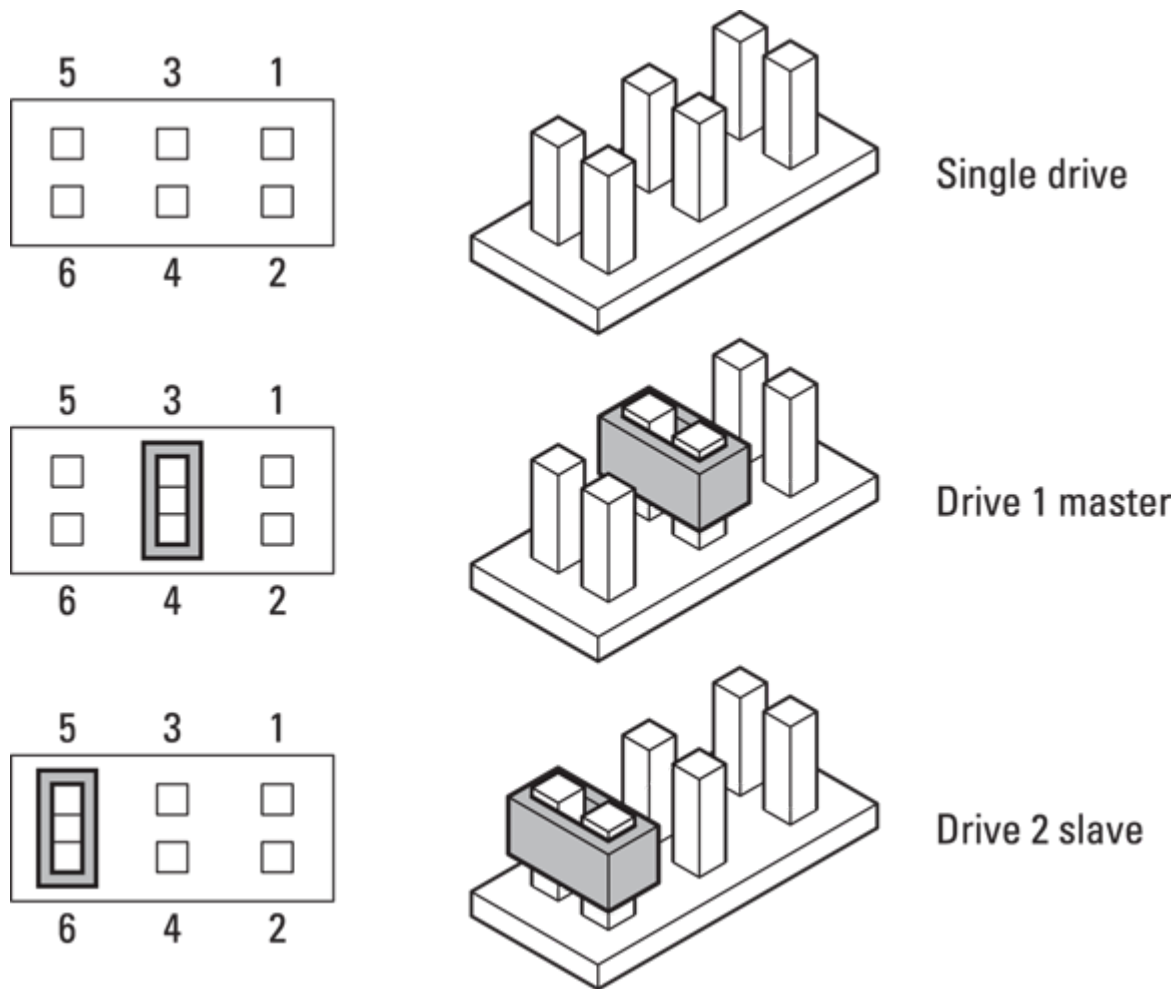
data on behalf of both drives. The other drive is designated as the *slave*, which passes any information it wants to send to the processor up to the master. The master then forwards that information to the processor. [Figure 5-8](#) illustrates a multidrive system.



**FIGURE 5-8:** One drive is configured as the master, and the other is configured as the slave.

To configure the master/slave relationship, you have to configure the jumper settings on the drives. The idea of the procedure is similar for all drives, but because the actual jumper setting might be different for each type of drive, the best thing to do is review the documentation for the drive.

Most hard drives today have the jumpers labeled as Master and Slave. Configuring these drives is usually pretty straightforward. You place the jumper on the master setting for the drive you want to be the master of the chain (meaning that this drive will communicate with the processor directly), and you place the jumper to the slave setting for the drive you want to configure as the slave. The slave drive receives instructions from the master. [Figure 5-9](#) displays master and slave jumper settings.

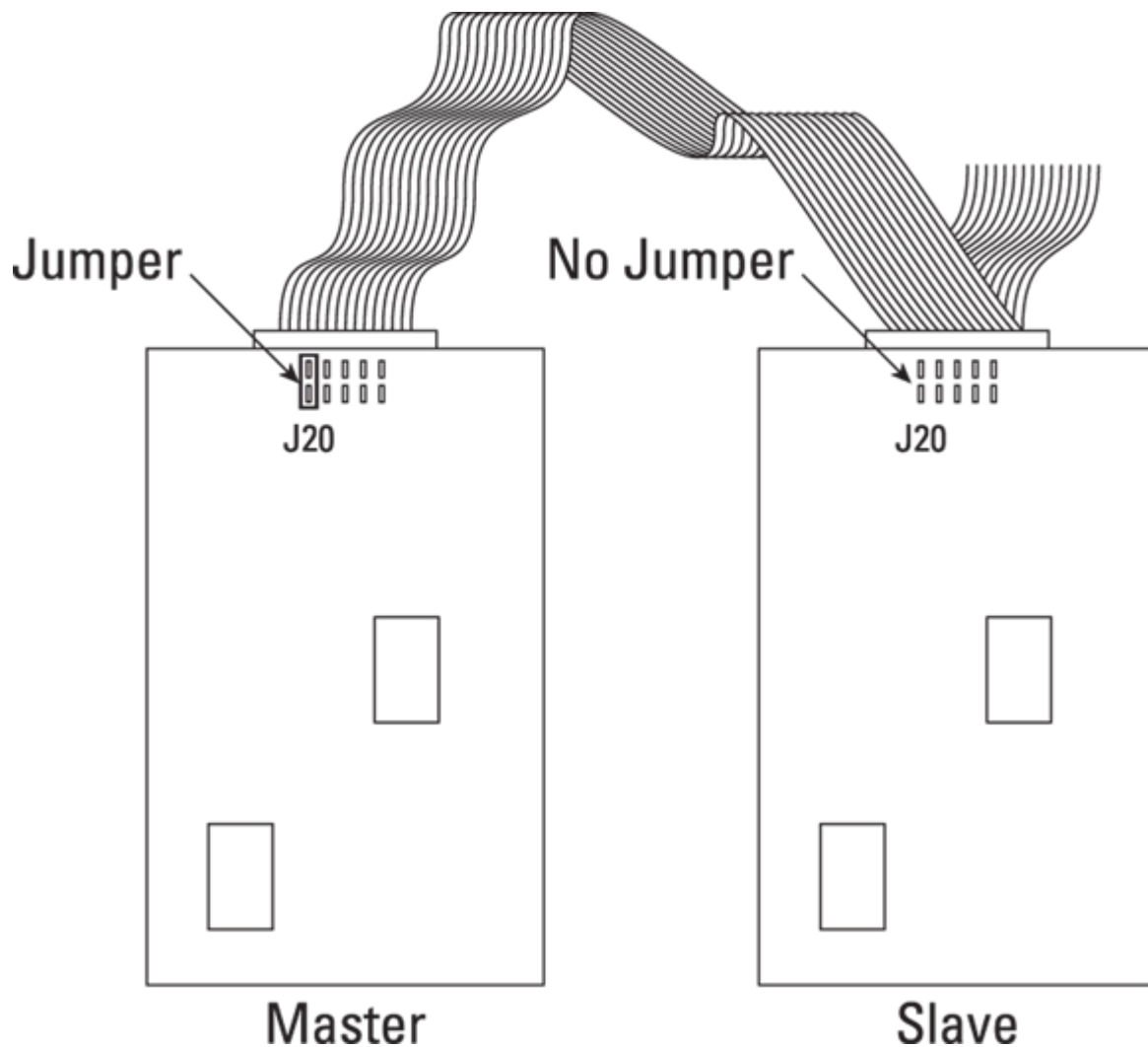


**FIGURE 5-9:** Adjust the jumpers to set one drive as a master and the other as a slave.

After you have decided which drive will be the master and which drive will be the slave, you will need to adjust the jumper on each drive to set the appropriate setting. For the hard disk that will be master, you will move the jumper to the master setting and for the drive that will be the slave, you move the jumper to the slave setting. Also note that you will configure an IDE CD-ROM or DVD the same way — as either a master or slave device in the IDE chain.

Many times, configuring your drives in a master/slave setup might not be as easy as it looks. What do you do when you cannot see a specific master or slave jumper setting? Many manufacturers place documentation on the back of the drive telling you how to configure the drive for master and slave setups. Unfortunately, this was not the case on a drive I had to configure in the office one day. So I went to the manufacturer's website

and found out that this drive had a jumper labeled J20; the website documentation stated that if the drive was the only drive or was the master in a dual-drive configuration, the jumper (J20) should be set. If the drive was the slave in the dual-drive configuration, the jumper (J20) should be removed. [Figure 5-10](#) shows the configuration for this example.



**FIGURE 5-10:** Looking at an additional jumper configuration for a dual-drive setup.



**REMEMBER** The moral of the story: If you can't find the jumper settings on the drives themselves, check out the drives' documentation or go to the manufacturers' websites.

If you end up supporting older systems, you will most likely end up installing Serial ATA (SATA) drives. By contrast, IDE, which supports up to four devices instead of two, is considered an “ancient” disk technology at this point and is included in the book mainly for historical reference.

Old computer systems have two IDE connectors on the motherboard: the primary IDE connector and the secondary IDE connector. Each connector can have two devices configured in a master/slave relationship, for a total of four devices. Typically, the devices can be hard drives or DVD devices. The steps are the same for configuring master and slave relationships for a hard disk, CD-ROM, and DVD because they are all considered IDE devices. Typically, you configure the CD-ROM or DVD as the slave, but you could also make it the master device on the second IDE connector.

After configuring the jumpers on the drive, power-on the system. The computer should recognize the additional drive and take you into the CMOS setup program. When you review the CMOS settings, you should notice the new drive. If you do not see the new drive, verify the master and slave settings, and maybe even switch the roles of the drives and try again.

## *Learning How SCSI Works*

You won't find traditional SCSI or serial-attached SCSI (SAS) hard drives in consumer computers. Instead, you find SCSI technology almost exclusively on server hardware and stand-alone disk arrays.

### *SCSI overview*

*SCSI* is an acronym for Small Computer System Interface. The important part of this term is *small computer*, meaning that SCSI has its own brain — the *SCSI adapter* — that handles the SCSI environment. This SCSI adapter (also known as a *SCSI card* or *SCSI controller*) is responsible for managing all SCSI devices and controlling the conversation on the SCSI chain.

SCSI technology has many advantages over IDE technology, such as

- » **The types of devices supported:** SCSI supports a multitude of devices, including hard drives, CD-ROMs, scanners, printers, and tape drives, to name just a few. This is a huge benefit because originally IDE typically supported only hard drives and CD-ROMs.
- » **The number of devices supported in a single SCSI chain (also known as a *SCSI bus*):** Original versions of SCSI supported as many as eight devices in the chain, but one of those devices is the SCSI card added to the computer to give you the capability to use SCSI.



**REMEMBER** IDE allows only two devices in the chain, and EIDE supports four devices. With SCSI, you are not only allowed to have more types of devices but also to have more of those devices!



**FOR THE  
EXAM**

Original SCSI supports as many as eight devices in the chain. However, if the A+ exams ask how many devices can be *attached* to a SCSI adapter, the answer is seven. If the test asks how many devices can *exist* in the SCSI chain, the answer is eight because the card counts as one of those devices. Remember to watch the wording of the questions closely.

- » **The performance of SCSI over IDE devices:** Original SCSI devices don't compare in the performance category with EIDE devices, but some of the later SCSI technologies, such as SCSI-2 and SCSI-3, can outperform IDE and EIDE.

I give details about transfer rates of the different types of SCSI devices in the “[Types of SCSI](#)” section, later in this chapter.



**TIP**

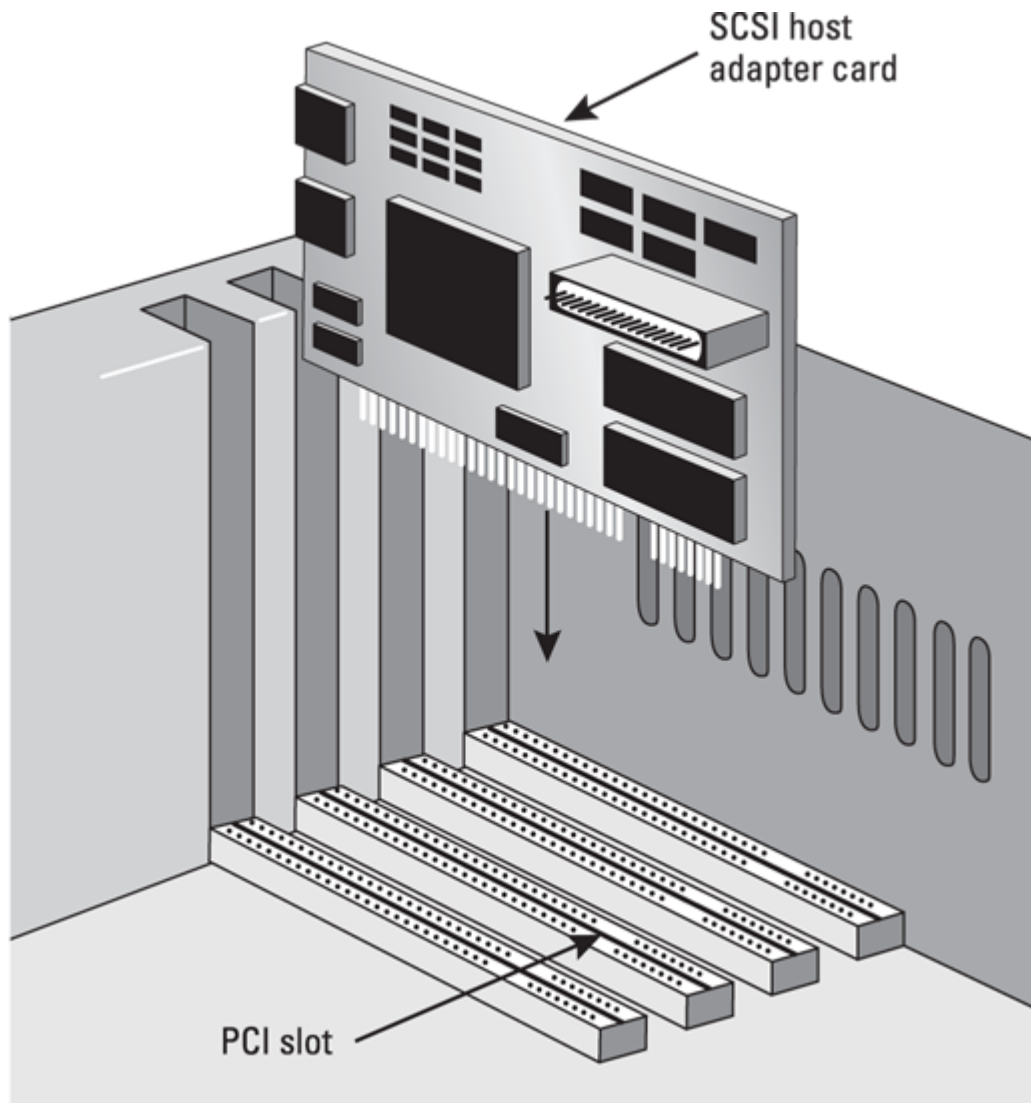
For the remainder of this chapter, assume that you are dealing with original SCSI, also known as SCSI-1. In the “[Types of SCSI](#)”

section, I discuss the newer types of SCSI.

### *Host adapter*

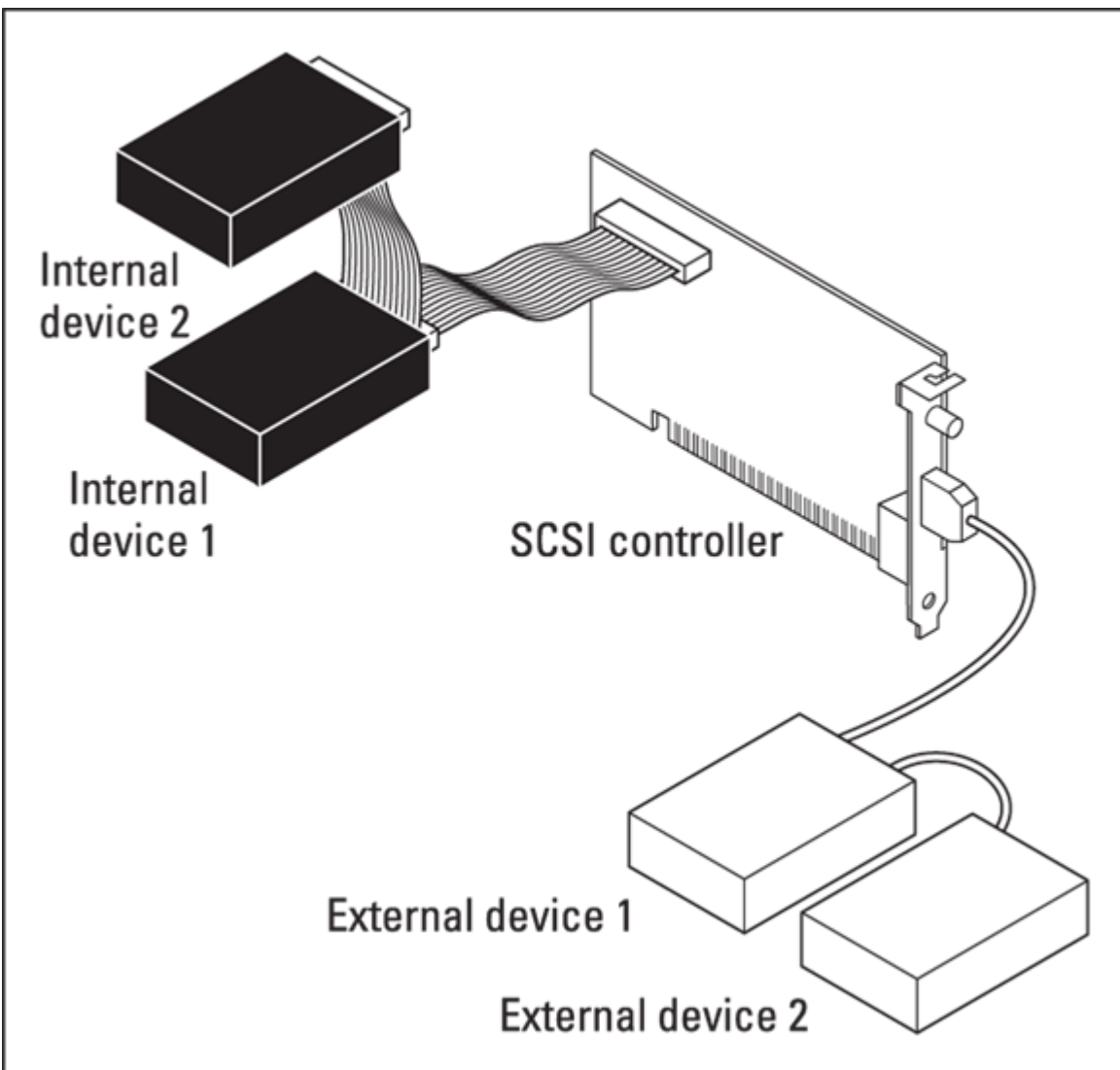
When you install SCSI devices, you first need to install the SCSI host adapter, which is an expansion card that you add to the computer so you can chain SCSI devices off the adapter. In essence, the SCSI host adapter is the brain of the SCSI bus; it acts as the controller for the SCSI bus.

[Figure 5-11](#) shows a SCSI adapter being inserted into an expansion slot in the system.



**FIGURE 5-11:** The SCSI host adapter.

The SCSI controller (adapter) is responsible for sending and receiving all information to and from the SCSI bus, just like the IDE controller. When the system has information for one of the devices in the SCSI bus, the system hands the information over to the SCSI controller, which then passes the information to the appropriate device in the chain. [Figure 5-12](#) shows a SCSI bus — made up of the SCSI host adapter (the SCSI controller) — along with two internal SCSI devices and two external SCSI devices.



**FIGURE 5-12:** Looking at a SCSI daisy chain.

The beauty of the entire setup is that the SCSI adapter in the computer is assigned resources, such as an IRQ and an I/O address. Each device in the



SCSI chain is not assigned these resources because all processor information passes to the SCSI controller, and the controller passes the information to the devices. This means that the system never talks to the devices directly, so each device does not require an IRQ and an I/O address.

When you purchase a SCSI adapter, first look inside your system to figure out what type of expansion slots are free. You will typically have some PCI slots, but you might have an ISA or EISA slot as well. The difference between these expansion slots is performance — PCI runs at 33 MHz, and ISA and EISA run at only 8 MHz. Also, PCI and EISA are 32-bit technologies, and ISA is only 16-bit. The bottom line is that if you have free PCI slots, you will probably end up purchasing a PCI SCSI adapter.

So the next big question is when the SCSI controller receives information for a particular device in the chain, how does it send the information to that device?

### ***Addressing***

Each device is assigned an internal address — a *SCSI ID* — in the SCSI bus. The SCSI controller knows the address of each device. When the SCSI controller receives information for a particular device, the controller references that device by its ID in the SCSI bus. This way, there's no confusion as to whom the data is destined for.

You are responsible for assigning the SCSI IDs when you connect each device to the SCSI chain. You assign an ID either by jumpers or DIP (dual inline package) switches if the device is an internal device, or by a spinner if the device is external. A *spinner* is an indicator on the back of the external SCSI device whose value you can change by pressing the button to increase or decrease the SCSI ID. [Figure 5-13](#) shows the back of an external SCSI tape drive and how to change the SCSI ID using the spinner.



**FIGURE 5-13:** Assigning a SCSI ID to an external device.



TECHNICAL  
STUFF

In [Figure 5-13](#), you can also see the type of connector used for external SCSI devices. This is a Centronics 50-pin connector.

If you are installing an internal SCSI device, you will most likely need to assign the SCSI ID by using jumpers. Internal SCSI devices have a jumper set with three pairs of jumper pins. The numeric values associated with these jumpers, although probably not shown on the drive, are 4, 2, and 1 (from left to right). [Table 5-3](#) shows this jumper setup.

### **TABLE 5-3 Jumper Block Settings**

<i>J2</i>	<i>J1</i>	<i>J0</i>
-----------	-----------	-----------

	<i>J2</i>	<i>J1</i>	<i>J0</i>
Numeric Value	4	2	1
SCSI ID 0	0	0	0
SCSI ID 3	0	1	1
SCSI ID 6	1	1	0

To assign the device a SCSI ID of 0, you would not add a jumper to any of the pins. This is shown in [Table 5-3](#) by having the off state (represented by 0) at each jumper location. Another example of setting a jumper ID is assigning the device a SCSI ID of 3: Jumper the J0 pins and the J1 pins, but not the J2 pins. This enables decimal values of 1 + 2. [Table 5-3](#) also shows what would happen if you want to set the SCSI ID to 6: Enable jumpers J1 and J2, which enables the decimal values of 2 + 4, while the jumper J0 has an off state.

The IDs you assign to each device are completely up to you, but note that the higher the number, the more important the device is to the SCSI bus. For example, if two devices need to send information through the bus at the same time, the device with the higher SCSI ID is always given priority. This is why the SCSI host adapter is usually assigned the highest number in the chain (usually 7 if the bus supports eight devices — the ID numbers start with 0).

So the host adapter is assigned an ID of 7, and a SCSI bootable hard drive is assigned a SCSI ID of 0, which is the SCSI ID that the controller automatically looks to in order to boot off a SCSI hard drive. Outside of that, you decide what the ID numbers are for each device. As a rule, give slower devices higher ID numbers so that they receive a higher priority in the SCSI bus. Devices with higher priority get access to the bus before lower priority devices.

### ***SCSI cabling***

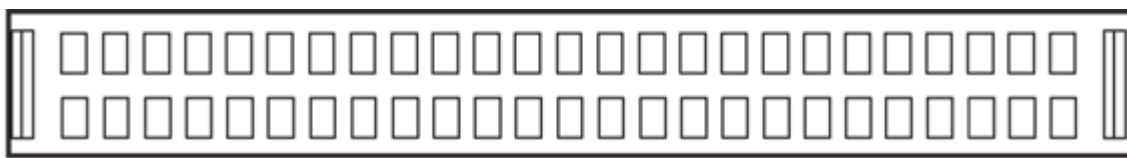
Different types of cabling are used to chain SCSI devices to the SCSI adapter. Internal devices use a 50-wire ribbon cable; external devices require a thick Centronics cable to connect to the Centronics 50 (typically

used by SCSI-1) or the Centronics 68 (typically used by wide SCSI-2 technologies or Ultra SCSI-3) connector on the back of the device.

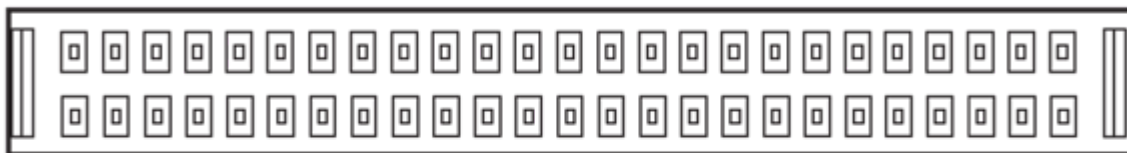


FOR THE  
EXAM

The different versions of SCSI use a large number of different cable types. [Figure 5-14](#) shows some internal SCSI connectors, and [Figure 5-15](#) displays a handful of external SCSI connectors. Be sure to be familiar with these cable types for the A+ exams.



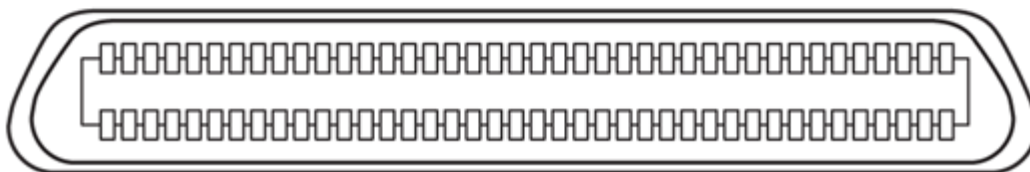
50-pin IDC female



50-pin IDC male

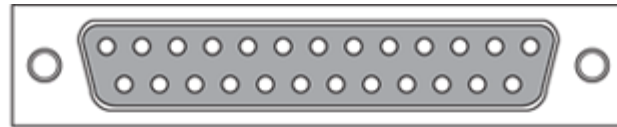


68-pin high density - male

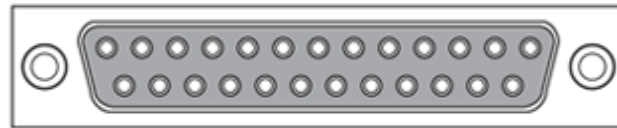


80-pin SCSI SCA connector

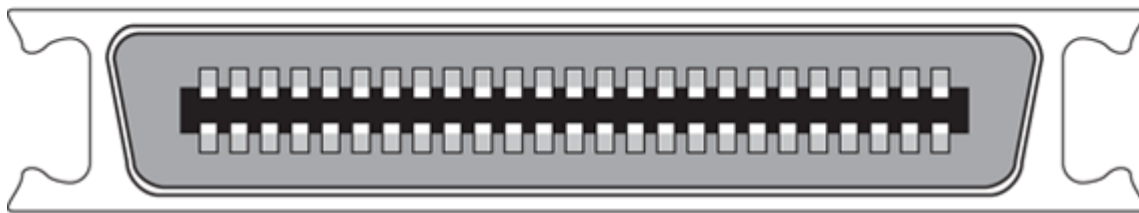
**FIGURE 5-14:** Looking at internal SCSI connectors.



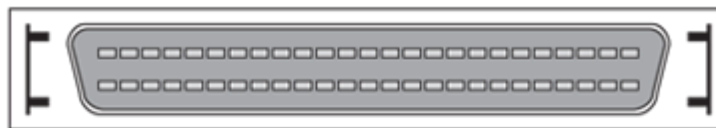
DB-25 female



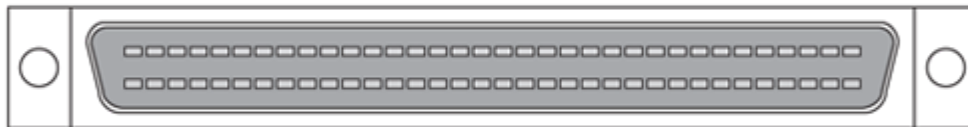
DB-25 male



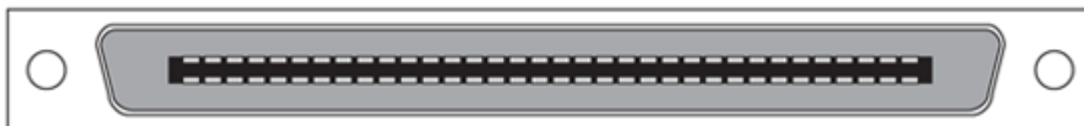
50-pin centronics



50-pin high density



68-pin high density

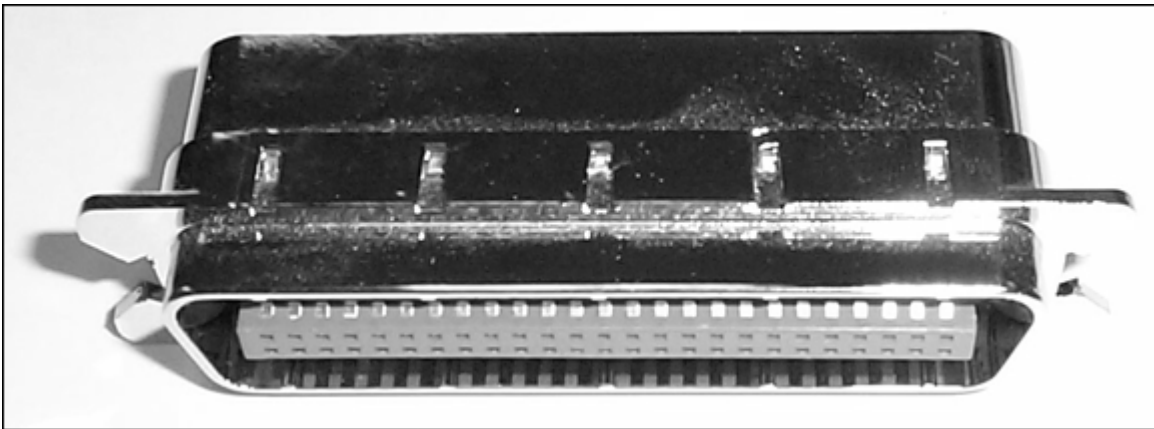


68-pin very high density

**FIGURE 5-15:** Looking at external SCSI connectors.

## *Termination*

Both ends of the SCSI bus must be terminated so that when a signal is sent down the SCSI bus, it is absorbed at the end of the bus by the terminator. If the signal was not absorbed, or removed from the bus with a terminator, the signal would bounce back and collide with other data on the bus. A collision would destroy the signal. The first device in the chain must be terminated along with the last device in the chain, the first device usually being the host adapter. If the device is an internal device, terminating might involve modifying jumper settings. If the device is external, a terminator will be added to the back of the device. [Figure 5-16](#) shows a terminator for external devices.



**FIGURE 5-16:** A SCSI terminator.

If your SCSI chain has a combination of internal and external SCSI devices, the card shouldn't be terminated because it is no longer the end of the SCSI chain. Instead, you should terminate the devices at either end of the SCSI chain.



TECHNICAL  
STUFF

Most SCSI cards today are self-terminating, so you typically will not need to terminate them manually.

### *Types of SCSI*

Over the past several years, SCSI technology has increased in performance to stay competitive with advances in IDE and EIDE. Newer versions of SCSI have amazing transfer rates, which is one of the reasons

why you find network servers using SCSI hard drives instead of EIDE devices. The following list outlines the key points about the different versions of SCSI:

- » **SCSI-1:** The original version of SCSI (SCSI-1) was an 8-bit technology with a transfer rate of 5 MBps. One of the major benefits of SCSI was that you were not limited to two devices in a chain like you are with IDE. SCSI-1 allowed you to have eight devices in the chain, with the controller counting as one.
- » **Fast SCSI-2:** Fast SCSI-2 increased the performance of SCSI by doubling the transfer rate. Fast SCSI-2 devices transfer information at 10 MBps. Fast SCSI-2 is still an 8-bit technology and supports eight devices in the chain.
- » **Wide SCSI-2:** Wide SCSI-2 doubled the 8-bit data path of SCSI to 16 bits. Doubling the width of the data path raised the transfer rate to 10 MBps, like Fast SCSI-2, but Wide SCSI-2 can support 16 devices in a chain.



FOR THE  
EXAM

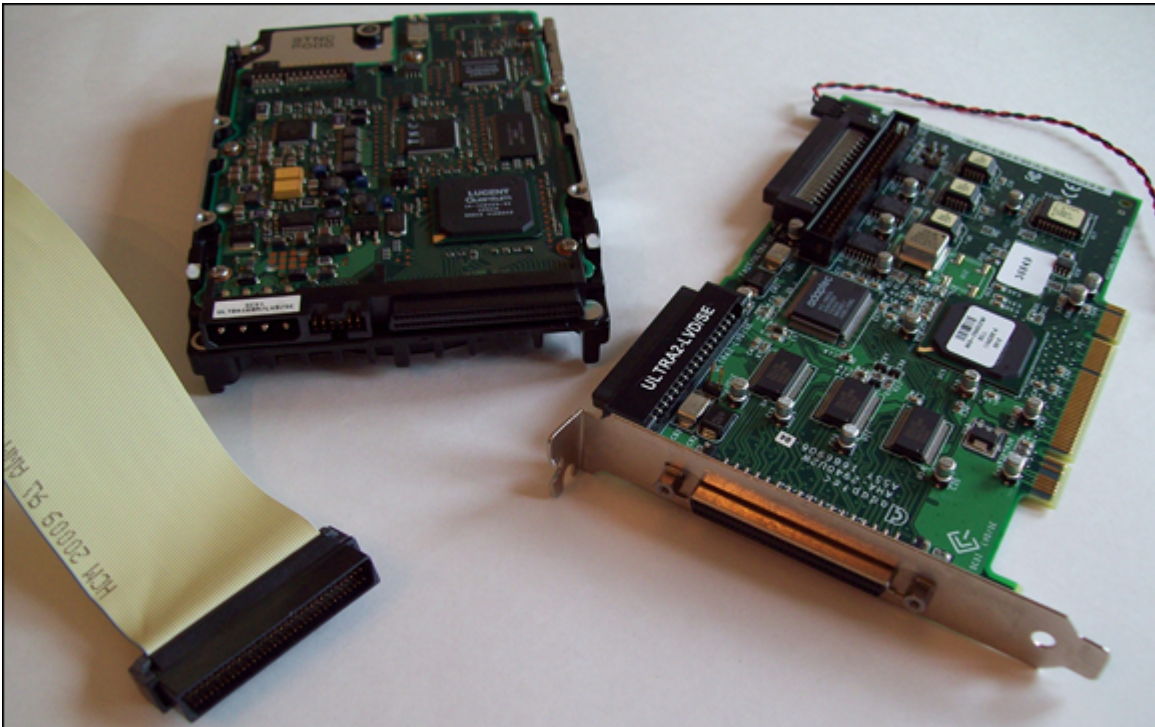
When trying to remember the difference between SCSI-1, Fast SCSI-2, and Wide SCSI-2, think of it this way. *Fast* implies speed, so the transfer rate is increased. *Wide* implies “wider” or bigger, which is the data path that has been increased; as a result, you also get a higher transfer rate.

- » **Fast Wide SCSI-2:** Fast Wide SCSI-2 is the combination of Fast SCSI-2 and Wide SCSI-2. The data path of Fast Wide SCSI-2 is 16 bits, the transfer rate is 20 MBps, and it supports 16 devices in a chain.
- » **Ultra SCSI:** Ultra SCSI takes the transfer rate of 10 MBps and doubles it again to 20 MBps! With Ultra SCSI, the bus width is only eight bits, and the number of devices that exist in the chain is eight.
- » **Ultra Wide SCSI:** Ultra Wide SCSI is Ultra SCSI with the bus width increased to 16 bits, and the number of devices in the chain is



increased to 16. The transfer rate of Ultra Wide SCSI increased to 40 MBps.

- » **LVD (Ultra2 SCSI):** *Low Voltage Differential (LVD)*, also known as *Ultra2 SCSI*, has a bus width of 16 bits and supports up to 16 devices. LVD is a popular SCSI version due to having a high transfer rate of 80 MBps. [Figure 5-17](#) shows an LVD adapter (or card) with a cable and hard drive.



**FIGURE 5-17:** An LVD SCSI card with hard drive and internal cable.



**FOR THE  
EXAM**

Be prepared to answer questions on the A+ exams about the different types of SCSI. I suggest memorizing the transfer rates of each type.

## *Installing SCSI devices*

If you understand the issues with SCSI, installing a SCSI bus is fairly simple. First, assign a unique ID number to each device. I usually perform



this step at the beginning so that when everything is connected, I won't have to play around figuring out how to change the ID of the devices. For more on assigning the IDs, see the section, "[Addressing](#)," earlier in this chapter.

When assigning the ID numbers, remember that you want to assign the bootable drive the ID of 0 because the SCSI host adapter automatically looks to SCSI ID 0 for a bootable device. You also want to enable the SCSI BIOS on the SCSI controller if you are booting off a SCSI hard disk. When you enable the SCSI BIOS, you won't need to install a driver for the card because the PC will recognize the device on startup. If you are booting off an IDE drive and using the SCSI disk as an additional drive, disable the SCSI BIOS and install a driver in the OS.

After you assign the ID numbers to each device, insert the SCSI host adapter into the expansion slot of the PC. After inserting the SCSI card, chain all devices.



FOR THE  
EXAM

When preparing for the A+ exams, know the different terms used for a particular technology. Another term for a *SCSI chain* is a *daisy chain*. When you chain devices, you create a daisy chain.

When you have the devices chained, make sure that each end on the SCSI bus is terminated. If the last device is an external device, put the terminator on the end of the device. If you are installing internal devices, check the documentation on the internal devices to find out what jumpers to set.

At this point, the IDs are configured for each device, the SCSI card is inserted into the PC, and the devices are connected to the card to create a SCSI bus. The SCSI bus is also terminated at either end. Before installing the driver for the SCSI card in the operating system, review the steps to install a SCSI device one last time. To install a SCSI bus, follow these steps:

- 1. Assign unique IDs to each device.**

2. **Install the SCSI host adapter into the expansion slots.**
3. **Chain devices to the SCSI host adapter.**
4. **Terminate the SCSI bus at both ends of the chain.**
5. **Install the driver for the SCSI card if you are not booting off the first hard disk.**

After you connect the hardware for the SCSI chain, you need to load a driver in the OS for the SCSI host adapter. After inserting the SCSI card and powering-on the Windows OS, Plug and Play should kick in, asking for the driver of the new hardware. If Plug and Play does not kick in, you can run the Add a Device Wizard in Windows 10 by opening the Control Panel, navigating to Devices and Printers, and clicking Add a Device from the toolbar.

## *Understanding Serial ATA*

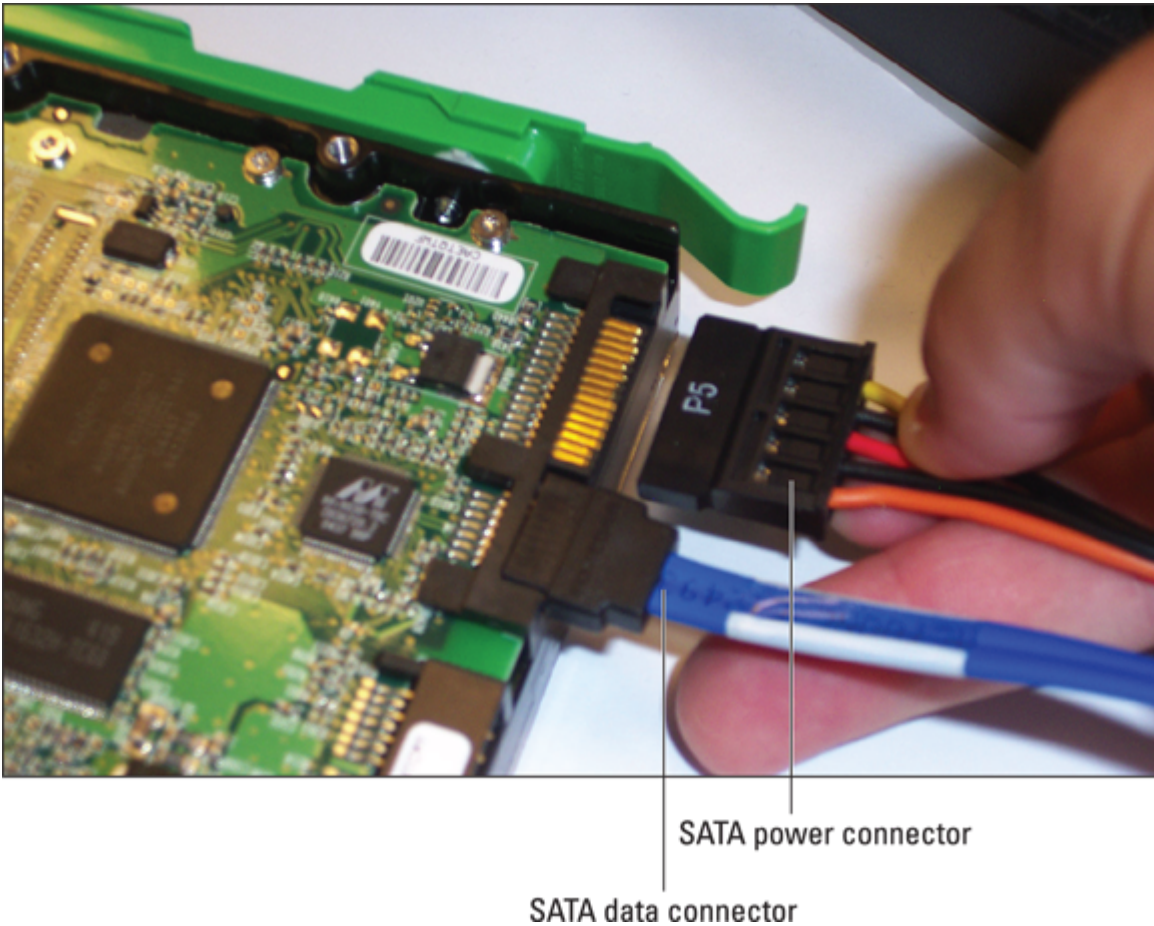
IDE technology has been around for many, many years, and there has been a big need for a change in hard drive technology. That change came as a new hard drive interface called serial ATA (SATA). IDE is a parallel technology (PATA), and although SATA is a serial technology, it offers great speed and other benefits. SATA is also a lot faster than IDE — approximately 30 times faster, with original speeds of 150 MBps and speeds of 2,000 MBps for SATA 3.2.

One of the first benefits of SATA is that it is a *hot-swappable* technology, meaning that you can add or remove drives from the system without shutting down the system. This is a huge benefit when you look for RAID solutions for servers that you don't want to spend a lot of money on — like a server for a small company. (For more on RAID, see the section “[A Quick Tour of RAID](#),” later in this chapter.)

Another benefit of SATA is in the cabling. Because SATA is a serial technology, the cables can be longer than your typical IDE ribbon cables. I don't know how many times with IDE I had to switch the CD-ROM and my second hard drive around just so the ribbon cable could reach. SATA

cables can be 39 inches long, but the maximum distance for IDE is 18 inches.

The other benefit of the cabling with SATA is that it uses only 7 wires, as opposed to the 80 wires used in newer IDE drives. The benefit here is that it allows for better airflow in the system, which results in a cooler system. [Figure 5-18](#) shows a SATA drive and cable.



**FIGURE 5-18:** A SATA cable and power connector connecting to a SATA drive.

With IDE, you have to master and slave the drives when you want multiple IDE devices. Yet another benefit to SATA is that there is no mastering and slaving of devices because you can only connect one SATA device to a single connector, or channel. The reason this is a benefit is because when installing a drive, you don't need to have knowledge of mastering and slaving devices — you simply connect the SATA device to the system!

SATA has all but replaced drive technologies like EIDE and SCSI, and currently has three versions:

- » **SATA v1:** 150 MBps transfer rate
- » **SATA v2:** 300 MBps transfer rate
- » **SATA v3:** 600 MBps transfer rate



**REMEMBER** If you want two SATA drives, you need two SATA connectors — and don't forget that you can get cards to give you more connectors, allowing you to install additional SATA devices.

One last note on SATA: Your BIOS offers a SATA *operation mode* setting that you may want to check. If you want the controller to support old PATA drives, you can set the operation mode to *parallel mode* (also known as *compatibility mode*). If you are using SATA in the system, set the operation mode to *AHCI* to leverage the benefits of SATA; this also supports the SATA drives in a RAID configuration. Most systems also have a *RAID mode* if you know you are configuring the SATA systems in a RAID configuration (use AHCI if you are not sure).



**ON THE  
WEB**

Lab 5-1 demonstrates how to install a SATA drive. Lab 5-1 can be found on the companion website at

[www.dummies.com/go/aplusaio](http://www.dummies.com/go/aplusaio).

## ***eSATA drives***

eSATA — *external SATA* — allows for external hard drives to connect to a system over a SATA port instead of the typical USB or FireWire port. In the past, external drives were enclosures that held SATA drives, but the interface to connect the enclosure to the computer used USB or FireWire. This created overhead as the SATA interface is translated to USB or FireWire, which is slower than SATA. With eSATA connections on the

motherboard, you can connect to the external drive using eSATA, thus leveraging SATA speeds with no translation drawbacks!



**TIP** You should always have at least one USB external hard drive enclosure (along with screwdrivers) in your troubleshooting toolkit. I cannot count how many times I've used them to restore files from a customer's old computer to a new one.

An eSATA device requires its own power source (it is an external device) and can have an external SATA cable length of 2 meters. eSATA cable is specially designed to help prevent electromagnetic interference (EMI). eSATA cable has also been designed to handle more than 5,000 times of adding and removing of the drive; the current internal SATA cable is suited for only 50 insertions and removals. [Figure 5-19](#) shows an eSATA connector on a 1TB (terabyte) external hard drive.



**FIGURE 5-19:** An eSATA connector on an external hard drive.

## *A Quick Tour of RAID*

Redundant Array of Inexpensive Disks (RAID) defines the myriad ways in which you can combine two or more separate hard drives for the goals of I/O speed and/or data safety.

You'll find that enterprise server computers almost always employ hardware RAID controllers that take care of all the back-end operations

required to keep these multi-disk enclosures up and running. However, many contemporary operating systems, Windows included, provide the ability to create software-driven RAID arrays. Of course, you'd be correct in assuming that hardware RAID is almost always preferable to software RAID.

## ***RAID 0***

A RAID 0 stripe set involves two or more hard drives that are bound together into a single virtual disk volume. Data is written to the stripe set across the array instead of one disk at a time. This provides RAID 0 with a definite performance improvement over non-RAID storage simply because you're drastically improving data transfer per read or write cycle.

If RAID 0 has a fault, it's just that — it's not a fault-tolerant system. If one participating disk fails, you lose all data in the striped volume across the entire disk set. Always back up RAID 0 volumes religiously!

## ***RAID 1***

RAID 1 sets are called mirrored volumes because you mirror every disk I/O operation on the primary disk member to a second, separate disk called (appropriately enough) the *mirror* disk. Therefore, you implement RAID 1 when data recovery is foremost on your mind. For example, many systems administrators will mirror the system drive of their servers to recover from a boot problem with minimal downtime.

Depending on your RAID controller, you can configure the mirrored drive to automatically assume the role of primary member if that primary disk goes offline. For software RAID like what Windows has, manual administrator intervention is always required.

## ***RAID 5***

A RAID 5 disk array is called a stripe set with parity. This RAID type attempts to blend the benefits of RAID 0 with the data redundancy of RAID 1.

You need at least three separate hard disks to build a RAID 5 set due to the redundant parity data that's required. You also lose one disk's worth



of data. The good news, though, is that a single drive failure won't destroy the data on the RAID 5 volume. You can simply replace the failed disk and let the RAID controller rebuild the RAID 5 volume by using the stored parity data. Pretty cool!

The “Achilles’ heel” of RAID 5 is that it cannot recover from a multi-drive failure. For that advanced scenario, we have hybrid RAID levels like RAID 10.

## ***RAID 10***

The name “RAID 10” is somewhat of a misnomer. Technically, RAID 10 should be written RAID 1 + 0, which denotes a striped set made from mirrored drives. This type of RAID array can survive multiple drive losses as long as no mirror partner loses all its members.

# ***Using Removable Storage***

Not all data storage is hard-wired to the system. *Removable storage* is the term used for storage media that you take away from the system with you.

## ***CD-ROM/CD-RW***

A *compact disc-read-only memory (CD-ROM)* is an optical storage technology that uses a laser to read and write data. Originally, as the name implies, one could only read from CD-ROMs. CD-ROMs have essentially gone the way of the dodo; DVD media is by far the standard nowadays.

Originally, CD-ROMs stored 650MB of data and could store 74 minutes of music, but today's CD-ROMs store 700MB of data or 80 minutes of music. CD-ROMs are written to from the inside out. If you look at the bottom of the CD-ROM, you see the lines indicating where data was written, which is very useful information if you ever pick up a CD and wonder whether it has been written to.

The speed (transfer rate) of the CD-ROM, measured in multiples of 150 KBps, is indicated with an *X*. For example, an old 1X (pronounced “one times”) CD-ROM had a transfer rate of 150 KBps, and an 8X has a



transfer rate of 1200 KBps ( $150 \times 8 = 1200$ ), and a much faster 48X has a transfer rate of 7200 KBps.

For many years now, CD drives are writeable: If you want to *burn* your own CD you can if you have a CD burner. (Writing to a CD is often called *burning a CD*.) This makes CD drives much more popular than the older floppy drives because of the amount of information you can store on the CD — a great solution for backing up your data!

The two types of writeable CDs are *CD Recordable (CDR)* and *CD ReWritable (CD-RW)*. The difference between them is that you can write to CDR only once, but you can reuse a CD-RW many times by reformatting the CD and starting again.

CDR speeds are shown in a format like 4 x 24: The first value is the record speed, and the second value is the read speed. Each value is multiplied by the 150 KBps to calculate the record and read speed. CD-RW displays three values to indicate the speed of the device: write speed, rewrite speed, and read speed — for example, 4 x 4 x 24.



FOR THE  
EXAM

A CDR is an example of a *write once read many (WORM)* disc.

Remember for the A+ exams that the CDR speed is displayed with the record speed showing first and then the read speed (4 x 24). CD-RW displays the speed as the write speed, rewrite speed, and read speed (4 x 4 x 24).

You can write to a CDR multiple times, but you cannot overwrite areas of the disc that have already been written to. With a CDR, writing to it many times appends the additional write operations information to the end of the CDR. Each burn operation that you perform is a *session*, and most writeable CD drives today support multiple sessions. For example, say you back up your pictures to CD and use only 350MB of space on the CDR. You can write more data to the CD with the remaining space at a later time. With the cost of CDRs being so low nowadays, I typically don't bother. I burn a CD, label it, and then file it.

When writing to a CD, the process is not done magnetically like it is with hard drives. As I mention earlier, the write operation is performed with a laser. The CD has a chemical-dye layer mixed with a thin reflective layer. When you write to the CD, the chemical layer is heated with the laser to create a solid state at that location. These locations reflect less light, and the different patterns of reflection create the data on the disk.

Many CD burners (used to write to CDs) come as combo drives that can burn CDs and *read* DVDs. The key point to remember about these combo drives is they cannot *write* to DVDs.

## ***DVD/DVD-RW***

*Digital versatile discs (DVDs)* are similar to CDs in the sense that they are another type of optical storage, but DVDs store a lot more data. The typical DVD stores 4.7GB of data. Some DVDs (unlike CDs) can store data on both sides of the disc, and newer DVDs even store data on different layers on the DVD. This allows the DVD to store more than the 4.7GB, depending upon the DVD standard. [Table 5-4](#) describes the different DVD standards.

**TABLE 5-4 DVD Standards**

<b><i>Standard</i></b>	<b><i>Specifications</i></b>	<b><i>Total Storage Space</i></b>
DVD-5	Single-sided, single layer	4.7GB
DVD-9	Single-sided, double layer	8.5GB
DVD-10	Double-sided, single layer	9.4GB
DVD-18	Double-sided, double layer	17GB

The transfer rates of DVDs are measured in a similar fashion to CD-ROMs but the transfer rate is 1.35 MBps for each times (X). For example, if you have a 2X DVD-ROM, it has a transfer rate of 2.70 MBps. An 8X DVD-ROM has a transfer rate of 10.80 MBps.



TECHNICAL  
STUFF

Double layer, also called dual-layer, discs store more data than single layer optical storage because you can write two separate data streams to the disc. Technically, these data streams are dye layers; you can see the color difference when you inspect the bottom of a “burned” DVD-DL disc.

## ***Blu-ray discs***

Blu-ray discs are popular items today in the video world because they offer the capabilities of high-definition (HD) video. Blu-ray has much better quality than DVD.

Blu-ray, created by Sony, was named after the fact that a blue laser is used to read and write to the Blu-ray disc. (DVDs use a red laser.) Not only does Blu-ray offer HD video, but it also stores more information than a DVD. Blu-ray discs can store up to 25GB of data for a single-layer disc, but can store up to 50GB of data for a double-layer disc!

Blu-ray discs also have a faster transfer rate than DVDs. DVD speeds could be calculated by taking the speed indicated and multiplying it by 1.35 MBps, but a Blu-ray disc has a multiplier of 4.5 MBps!

## ***BD-R and BD-RE***

Blu-ray discs are like DVDs in that they have recordable versions as well. Blu-ray disc recordables (BD-Rs) are Blu-ray discs that can be written to once, while Blu-ray disc recordable erasables (BD-REs) can be erased and then written to many times.

## ***Solid state drives***

Solid state drives (SSDs) use a totally different approach to storing data on the drive than conventional drives, which use magnetic states to store the data. Solid state drives do not have any moving parts such as platters or read/write heads; they simply store data permanently to a huge block of memory. On mid-tier computers and higher, you’ll find SSDs are pretty standard.

### ***Flash drives/thumb drives***

*Flash drives*, also known as *thumb drives* or *memory sticks*, are the popular method for carrying data from computer to computer. Flash drives, which can store anywhere from 64MB to multiple gigabytes of information, are relatively inexpensive.

Flash drives are USB devices that you simply plug into the USB port on the computer. Plug and Play kicks in, detects the device, and assigns the drive a letter in Windows 10 File Explorer. To access the flash drive, you simply double-click the drive in File Explorer and open, copy, and move files as you wish. [Figure 5-20](#) shows a flash drive.



**FIGURE 5-20:** A flash drive uses a USB connection to interface with the computer.

### ***Hybrid drives***

A hybrid drive (also called an SSHD drive) is a traditional mechanical hard disk drive that includes on-board flash storage for use as cache. Thus, drive performance is improved because the disk controller has high-speed access to the SSD data cache.

### ***SD cards***

Multimedia devices, such as MP3 players and digital cameras, support adding memory to the device by using *CompactFlash cards* or *Secure Digital (SD) cards* (as shown in [Figure 5-21](#)).



**FIGURE 5-21:** A CompactFlash, SD card, and SD card carry case.

Related to the SD card standard is the embedded MultiMediaCard (eMMC). These tiny packages incorporate flash memory plus a controller and are typically installed permanently as a non-volatile memory system for mobile phones and tablets.

CompactFlash (CF) cards have been very popular but have been replaced by SD cards. SD cards are used by a number of types of devices such as digital cameras, laptops, printers, MP3 players, and PDAs to name a few types of devices. SD cards are a great way to carry your data from one device to another.

SD cards store data up to 4GB, but a newer SD format — Secure Digital High Capacity (SDHC) — can store information up to 32GB or even 2TB (!). The problem is that SDHC cards cannot be read by devices that only support SD cards. For a device to be able to read an SDHC card, the device must be compatible with SDHC. This is important to remember when you purchase an SD card for your camera. The SD and SDHC cards are the same physical size and appear the same; look for the label indicating SDHC on the SDHC card.

You should be familiar with a number of other types of removable media for the A+ Certification:

- » **SDXC:** The secure digital extended capacity (SDXC) cards allow up to 2 TB of space for the SD card.
- » **Mini-SD:** Mini-SD cards are smaller than the SD and SDHC cards, with dimensions of 21.5 mm × 20 mm × 1.4 mm.
- » **Micro-SD:** Micro-SD is the smallest type of non-volatile memory you can find today. Micro-SD memory cards are commonly used with mobile devices such as phones and tablets. You can also purchase an adapter that allows you to connect the micro-SD in a regular SD slot so that it can be used with a PC.
- » **xD:** Extreme Digital (xD) cards are older memory cards used in cameras that ranged in sizes from 16 MB to 2 GB. xD competed with other technologies such as CompactFlash and is no longer being used in newer cameras.

## **M.2**

This standard, formerly known as Next Generation Form Factor (NGFF), defines a new way to mount expansion cards inside a computer chassis. Specifically, M.2 allows easier expansion of SSDs by reducing the form factor size and offering higher throughput speeds.

M.2 SSDs are so small, in fact, that they dwarf the size of traditional 2.5-inch SATA drives. Some technicians jokingly describe M.2 SSDs as “sticks of gum.”

## *NVMe*

Non-Volatile Memory Express is a communications standard developed by a consortium of SSD drive manufacturers. The purpose of the standard is to help SSD drives act more like RAM in terms of access time and overall performance. NVMe SSD drives can read and write data four times faster than traditional SATA SSDs.

## *External hard drives*

External drives are just as popular as flash drives today. Like flash drives, an external drive uses a USB connection, but could also allow you to connect the drive through FireWire or eSATA. External drives allow you to store hundreds of gigabytes, even a terabyte, of data. These are great solutions to add more space to a laptop computer or desktop PC.

## *Tape*

A popular type of media for data is *tape*, which is typically used to store backup copies of data. This copy of the data stored on tape is used to bring the data back if the hard drive fails. Different types of tape drives are popular today:

- » **Quarter-inch cartridge (QIC):** QIC — one of the oldest and most popular tape standards — supports many different tape sizes. The QIC size depends on the standard, and each standard is labeled similar to QIC-80 — the QIC tape that supports 80MB of data. Other examples are QIC-40 (40MB tapes) and QIC-5210 (25GB tapes).
- » **Travan:** Travan is a tape drive standard based on the QIC standard but supports compression. Travan is typically more expensive and can store from 400MB to 8GB of data or more. Examples of tape sizes in this standard are labeled as TR-1 (stores 400MB of data) and TR-4 (stores 8GB of data).
- » **Digital Audio Tape (DAT):** DAT drives store data in a digital format and use two heads: one for reading data and the other for writing data. DAT drives use a standard called *Digital Data Storage (DDS)* to store data. Examples of DDS tapes are DDS-1 (stores 2GB of data), DDS-2 (stores 8GB of data), and DDS-4 (stores 40GB of data).



# *Troubleshooting Hard Drives and RAID Arrays*

Let's close the chapter by quickly reviewing some of CompTIA's best practices for resolving problems with mechanical hard drives, solid-state hard drives, and RAID arrays. To do this, I list a number of common symptoms, followed by their typical resolution:

- » **Read/write failure:** If you receive read/write failures only occasionally, then I recommend (a) backing up the affected files; and (b) running CHKDSK to repair any bad sectors on your hard drives.
- » **Slow performance:** A mechanical hard drive may be slow due to fragmentation. A USB external hard drive may be slow if the device is plugged into an older USB port. For instance, a USB 3.0 hard disk that's plugged into a USB 2.0 port can perform I/O only at USB 2.0 speeds.
- » **Loud clicking noise:** This is a bad sign that typically signifies a hard drive's end of life. It's crucial that you back up the data from a clicking hard drive and replace it as soon as possible.
- » **Failure to boot:** This problem is tremendously vague, but inspires me to look below the surface to determine exactly why a bootable hard disk won't start.
- » **Drive not recognized:** This problem most likely indicates that the boot record on the disk has become corrupted or was deleted. In Windows, boot to Windows RE and run `bootrec` to fix this problem.
- » **OS not found:** This problem signifies that you once had a working operating system, but don't any longer. In Windows, this error can be remediated easily enough by performing the emergency repair process by using your Windows installation media and Windows RE.
- » **RAID not found:** The first thing I'd check to resolve this error are all the hard disk connection cables. Failing that, I'd then verify that the



RAID device driver software is still present on the computer and re-install if necessary.

- » **RAID stops working:** This problem could indicate that the RAID controller hardware or software has become damaged.
- » **Proprietary crash screens:** In Windows, this is called the “Blue Screen of Death,” or BSOD for short. In macOS, you see the “Spinning Beach Ball of Death.” Either way, the operating system presents a special screen to indicate that the OS has experienced a crash that can be remedied (it is hoped) by performing a system restart.
- » **S.M.A.R.T. errors:** Hard drives with S.M.A.R.T.—alerting technologies are cool because the purpose of S.M.A.R.T. is to give you advanced warning of imminent drive failure. When you see this kind of error, back up all data from the drive and replace it immediately.

## *Getting an A+*

This chapter illustrates the importance of hard disk management and the utilities used to perform that management. The following are some key points to remember when managing hard disks:

- » EIDE devices are slower than SCSI and SATA and only support a total of four devices in the configuration, with two devices per EIDE chain.
- » EIDE devices are configured in a master/slave configuration by setting jumpers on the drives.
- » SCSI devices need to have a host adapter and unique IDs, and the SCSI bus must be terminated at both ends.
- » SATA drives are much faster than EIDE and support hot-swapping. Each SATA port on the motherboard supports connecting a single SATA drive.

- » CD-ROMs can store 700MB of data, while most DVDs are able to store between 4.7 and 8.5GB of data. Blu-ray discs can store between 25GB and 50GB of data!
- » An 8x DVD can transfer data at 10.80 MBps, while an 8x Blu-ray can transfer data at 36 MBps.

## *Prep Test*

### **1. What is the size of a sector on a hard disk?**

- (A) 512 bytes
- (B) 1K
- (C) 4K
- (D) 512K

### **2. How many devices can exist in an IDE chain?**

- (A) 1
- (B) 2
- (C) 3
- (D) 4

### **3. What physical component of the disk is responsible for reading and writing data on the disk?**

- (A) Platter
- (B) Sector
- (C) Cluster
- (D) Read/write head

### **4. What does DL mean in the acronym DVD-RW DL?**

- (A) Device Layer
- (B) Dual Layer
- (C) Disc Level

(D) Drive Letter

**5. In a SCSI chain, what devices are required to be terminated?**

- (A) The first device in the chain
- (B) The last device in the chain
- (C) Devices at either end of the SCSI chain
- (D) Any hard disk in the SCSI chain

**6. In a SCSI chain, what device should take a SCSI ID of 0?**

- (A) CD-ROM
- (B) The bootable (first) hard disk
- (C) The SCSI host adapter
- (D) Printer

**7. Which of the following is considered a hybrid RAID type?**

- (A) RAID 0
- (B) RAID 1
- (C) RAID 5
- (D) RAID 10

**8. Which of the following describes the cabling for internal SCSI?**

- (A) 40-wire ribbon cable
- (B) 34-wire ribbon cable
- (C) 50-wire ribbon cable
- (D) None of the above

**9. Which of the following best describes where the Master Boot Record is located?**

- (A) Last track on the disk
- (B) First track on the disk
- (C) First sector on the first track of the first side of the first platter

(D) First sector on the last side of the last platter

## Answers

1. **A.** A single sector on the disk is typically 512 bytes. A group of these sectors makes up a cluster, which typically could be 4K, 16K, or 32K. See “[Sectors](#).”
2. **B.** IDE supports only two devices in an IDE chain. EIDE improves on this limit by allowing four devices. Review “[IDE/ATA standard](#).”
3. **D.** The read/write heads are responsible for moving over the disk surface and writing data to the disk. A platter is one of the disk plates, a sector is where the data is written, and a cluster is a group of sectors. Check out “[Read/write process](#).”
4. **B.** The DL in DVD-RW DL stands for double layer. This means that the disc has typically double the capacity of a single layer optical disc. See “[DVD/DVD-RW](#).”
5. **C.** Devices at each end of the SCSI bus must be terminated. This is usually the SCSI host adapter plus the last device in the chain. Take a look at “[Termination](#).”
6. **B.** A bootable hard disk should take SCSI ID 0, and the host adapter usually takes an ID of 7. The other devices can be assigned any number in the chain as long as it is a unique number. Peek at “[Addressing](#).”
7. **D.** RAID 10 is an example of a hybrid RAID array because, in this case, you’re combining a RAID 1 set with a RAID 0 set. Check out “[RAID 10](#).”
8. **C.** An internal SCSI connector uses a 50-wire ribbon cable, an IDE device uses a 40-wire ribbon cable, and a floppy drive uses a 34-wire ribbon cable. Study “[SCSI cabling](#).”
9. **C.** The master boot record is the first sector on the first track of the first side of the first platter. Refer to “[Sectors](#).”

# Chapter 6

## Working with Power

---

### IN THIS CHAPTER

- » Understanding the features, functions, and installation of power supplies
  - » Identifying infrastructure power issues
  - » Managing surges, brownouts, and blackouts
- 

This chapter takes a look at two main items: power supply units (PSU) and uninterruptible power supplies (UPS). Power supplies should actually be called *power converters* because the largest single function they perform is a conversion of power from 120 volt (V) or 240V to something that can be used by the computer system.



**FOR THE  
EXAM**

The current exam objectives list the power supply voltages as 115V and 220V, so given a choice on the exam, these should be used; while North American voltage is rated at 120V, actual supplied voltages could be as low as 110V due to line issues. Other countries may provide standard voltages around 110V, 220V, 230V, or 240V, all with a similar voltage fluctuation.

As a CompTIA A+ Certified Professional, you will at least have to add a component to a computer that requires power from the power supply (such as a hard drive), and you will also probably be required to troubleshoot and replace a power supply in the computer system. The information in this chapter gives you all the technical specifications and connector types you will need to know about a power supply. Together with the troubleshooting chapter (Book 4, [Chapter 2](#)), you will have all the information that you need to know about power supplies.

# *Knowing the Basics of Power Terminology*

You should learn four terms that deal with power in computer systems: volts, ohms, amps, and watts. If you have a firm grasp on how they relate to each other, you can understand how power is measured and used within computer systems. Electrical current flows with the same principles that are used when water flows, so water is often used as an analogy for electrical current.

## *Volt*

A technical definition of a *volt* is a unit of electrical potential difference or the potential difference across a conductor when a current of one ampere dissipates one watt of power. In water terminology, voltage is represented by the pressure that is the water supply tank. This is a potential because unless you provide an exit path for water to leave the tank, this potential is not realized. If you increase the pressure in the tank, you increase the potential to supply water or power.

## *Ohm*

An *ohm* is a measure of resistance or electrical impedance. When comparing electricity with water, resistance is determined by the size or diameter of the hose or pipe that is used to supply water, where a smaller hose produces more resistance.

## *Amp*

An *ampere* (amp) is a unit of electric current or the measure of electrical flow. When referring to water, it is also the rate of water flow. There is a direct relationship between volts, resistance, and current: If you reduce resistance or increase voltage, you increase the current. This relationship — Ohm's Law — is represented by this formula:

$$I = V / R$$

where I is current (amps), V is voltage (volts), and R is resistance (ohms).

## *Watt*

The technical definition of a *watt* is that it is a unit of power, equal to one joule per second. If you equate this to water again, watts have you use flowing water to do something. If this water runs over a waterwheel, watts are the measure of how fast the wheel can be turned by the water. If you increase the current, the wheel is able to turn faster. The formula to calculate watts is

$$P = V * I$$

where  $P$  is power (watts),  $V$  is voltage (volts), and  $I$  is current (amps).

In general, when you are working with computer systems, you will be concerned with the voltage supplied by the outlet that you connect your equipment to, the current that your equipment draws from the outlet, and the power that is used by devices that are connected to the computer power supply.

## *Identifying the Purpose of Power Supply Units*



FOR THE  
EXAM

Remember the tasks and specifications listed in this section.

A computer's power supply is responsible for several tasks. The following list contains typical tasks and specifications related to power supplies:

- » **Conversion of voltage** from the building-supplied AC voltage to various DC voltages used by components inside the computer.
- » **DC voltage regulation** to provide a very small tolerance of error to the devices receiving the power. Typically, a  $\pm 5$  percent voltage differential is allowed through the specification for 12VDC, 5VDC, and 3.3VDC connections.

- » **Over-current protection (OCP)** specifies that the power supply should handle some level of abnormally high current to prevent fuses in the power supply from blowing unnecessarily.
- » **Input-under voltage** specifies that if the voltage being supplied by the building drops below the normal operating level, it should not cause damage to the power supply itself. It will, however, likely cause your computer to turn off. For a 120V power supply, this low voltage level is usually 100V, so at voltages below that level, the power supply will simply turn off.
- » **Energy Star** is a specification that defines how much power the power supply should provide to the computer components during reduced power states, such as when the computer is put to sleep or on standby.
- » The **power supply specification** might recommend or require the use of cooling fans, depending on the form factor of the power supply.
- » **Input supply voltage** (120V or 240V) might be static or configured via manual switching or automatic switching. Most currently available desktops, laptops, and power supplies have automatic switching, while some older systems may still have power supplies with manual switching. Check your product specifications and power labels for the supported input power specifications for values like 100V to 240V, 115V to 220V, or some other variation. Always check your input supply voltage if you are unsure.



**TIP**

If you do not see a manual switch on your power supply, read the input voltage range displayed on a label on the power supply, on the outside of the computer, or in the computer or power supply specifications to ensure that it does support your input voltage.

*Automatic switching* just means that the power supply will detect and use the voltage setting for the power that is supplied. These automatic switching power supplies are also referred to as *dual voltage power supplies*. As I discuss at the start of this chapter, if you increase the



voltage, you increase the current, and increasing the current would cause damage to your computer's internal devices. Thus, the power supply deals with the increase in voltage by reducing the current inside the power supply, which allows your computer's internal devices to have a consistent power level (voltage and current).

## *Identifying Power Supplies*

The most common type of motherboard that you will have to provide power to will be some form factor of the ATX family (see Book 2, [Chapter 1](#)) — and, because of that, some form of power supply compatible with an ATX motherboard will be required. In the following sections, I discuss the things that are common to all power supplies that are compatible with ATX motherboards. I also take a look at the different form factors for power supplies so that the many sizes and shapes of computer cases can be supported, from tower to small form factor (SFF) to slimline cases, and all sizes in between.



TECHNICAL  
STUFF

When the name *ATX power supply* is used properly, it refers to a power supply that provides power to an ATX motherboard, and it has very specific size characteristics. Many other power supplies (such as CFX, LFX, SFX, and TFX) have different size characteristics, but all provide power to the ATX family of motherboards. Each size and shape of power supply has its own specification. In this chapter, I talk only about power supplies that provide power to ATX motherboards, regardless of their size and shape. All these power supplies use the ATX-compatible main power connector, which makes them different from the older AT power supply used with older generations of motherboards.



TECHNICAL  
STUFF

To find out more about the specifications for power supplies for ATX motherboards, look at the Desktop Platform Form Factors Power Supply Design Guide document at

<https://www.intel.com/content/dam/www/public/us/en/documents/guides/power-supply-design-guide-june.pdf>.

The ATX power supply has undergone some basic changes in power that is supplied and in the format of the connectors. The current version of the ATX specification is 2.52. The biggest difference between the version 1.3 ATX specification and the 2.x ATX specifications is the use of a 24-pin main power connector used in the 2.x ATX specification, rather than a 20-pin connector under the 1.3 ATX specification.

With ATX power supplies having the same types of power connectors, one big difference between the power supplies you could purchase is how much power they provide to connected devices. The power supply rating refers to the total wattage that the power supply can provide to devices within your computer. Although ATX specification allows for power supplies to have ratings from 250 watts (W) up to large ones at 1600+W, most are typically around 500W to 800W. Lower wattages are available, too, but these usually follow the SFX specifications (sometimes called *microATX power supplies*), and these have power output down to 160W.



TECHNICAL  
STUFF

If you are shopping for a replacement power supply, you will see many items in the specification, like wattage rating and rails. You may be thinking that with so many power supplies on the market to choose from, you should likely get the one with multiple rails, since that must be better, right? Not necessarily, and this has proven to be an issue of great debate. Power supplies have one or more +12V rails. A *rail* consists of a power circuit connected to wires supplying the standard plug connections monitored by an OCP circuit. Think of

the circuits like the ones in your house, where the OCP is the circuit breaker on your power panel. In a single rail power supply, there is only a single circuit supplying power to the connected devices and a single OCP monitoring the rail for load, while multi-rail power supplies will have the total wattage supplied by several circuits, each with an OCP circuit monitoring the rail for load. For example, in my house, the kitchen may be one rail and the living room another rail. When I plug in a kettle in the kitchen and overload the rail (and trip the breaker), my television in the living room remains running. The OCP circuit keeps the whole thing from overloading, so in a multiple rail power supply, you will only lose a portion of the internal devices based on the rail they are connected to rather than all of them. But what good is your computer if only some of the components are running? Do not sweat discussions over rails; if one rail goes bad, then you are replacing the entire power supply unit.

The power supply rating required for any computer depends on the devices within the computer that need power. In most cases, bigger is better because systems that don't have enough power for devices can experience strange, intermittent problems (see Book 4, [Chapter 2](#)). [Table 6-1](#) provides a listing of some basic systems devices and power usage estimates as a guide to sizing up a power supply, but remember to always leave yourself some extra room.

**[TABLE 6-1](#) Power Consumption by Product**

<i>Device</i>	<i>Power</i>
PCIe video card	30–225W
AGP video card	30–75W
PCI video card	30–35W
AMD Athlon XP, 1.5 MHz–2.5 GHz	66–77W
AMD Athlon 64, 3.0 GHz–3.4 GHz	89W
AMD Athlon 64, dual-core, 3.0 GHz–3.4 GHz	125W
Intel Pentium 4, 2.2 GHz–2.4 GHz	80W–90W
Intel Pentium 4, 2.4 GHz–3.0 GHz	90W–105W

<b><i>Device</i></b>	<b><i>Power</i></b>
Intel Celeron Socket 478	45W–65W
ATX motherboard	40W–65W
PC133 RAM	12W
PC2100+ DDR RAM	10W
PC3200+ DDR2 RAM	7.5W
CD-ROM drive	20W
CD-RW drive	30W
DVD-ROM drive	25W
ATA hard drive, 5400 rpm	15W
ATA hard drive, 7200 rpm	25W
SSD	3–5W
Network card or modem	5W
Sound card	7–18W
SCSI controller card	25W
FireWire or USB 2.0 controller card	40W
USB device	5W
FireWire device	8W
CPU fan or case fan	2W

If you are replacing a power supply in a system that experienced a failure, you can get a replacement that provides the same amount of power or more. However, if you expect that your system has more devices than the power supply can support — or if you are building a custom system — you can follow these steps:

1. **Locate in [Table 6-1](#) any devices that your system is going to contain, then record the power usage.**
2. **Add up all the wattages and divide your total by 80 percent (0.8) to give your system some extra room to grow and to accommodate any items you might have missed.**

3. If you did not get a number that matches an available power supply rating, choose a power supply with the next highest power rating.



TECHNICAL  
STUFF

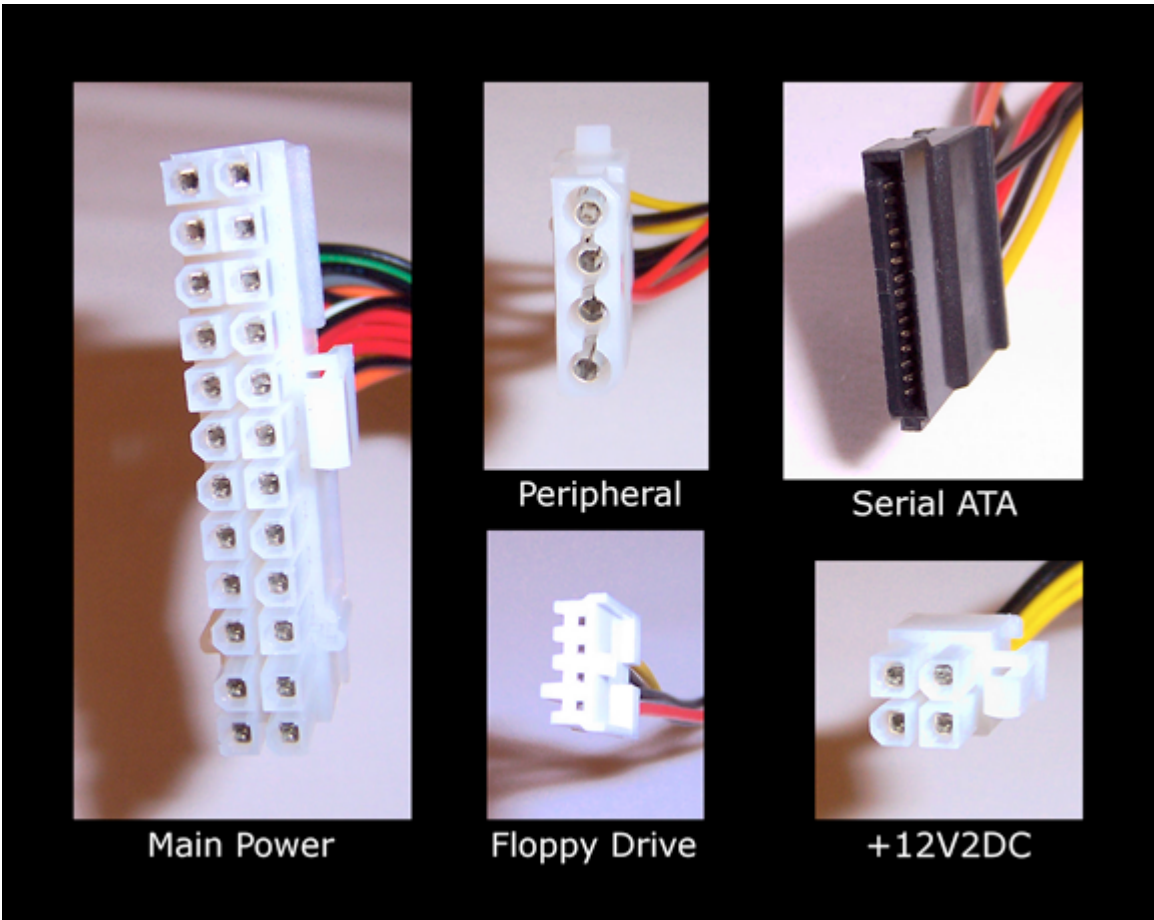
To assist you in adding up the wattages used by devices, you can find a number of PSU calculators on the Internet. These will make use of standard wattage requirements for devices and will get you close to your total without the need of digging through the technical specifications for your devices.

## *Power Connectors*

A computer uses many different types of power connectors. They include the main power, floppy, peripheral, 12-volt (+12V2DC), and serial ATA (SATA) connectors. When shopping for a power supply, you will find that there are two main categories: fixed cables and removable cables. Fixed configurations will have a variety of connectors hardwired to the power supply, while many manufacturers offer power supplies with a number of plugs along with a variety of cables, allowing you to only attach the cables which you need for the devices inside of your computer case. Typically, there is a very small price differential, and by being able to choose to only put some of the cables in your case, you improve airflow and do not have problem with what to do with a huge bundle of cables.

### *The ATX main power connector*

On power supplies, the ATX main power connector is a 24-pin Molex 39-01-2240 connector. In many cases, it is a 20+4-pin connector for backward compatibility with older, version 1.3 motherboards. This is a keyed connector, so you cannot connect it the wrong way without a lot of effort. You can see this and other connectors in [Figure 6-1](#).



**FIGURE 6-1:** Power connectors that may be used on power supplies.

[Table 6-2](#) lists the pin configuration and voltage supply for the 24-pin Molex main power connector. When troubleshooting faulty power supplies, you need to know what power is supposed to be supplied by each pin in the power connector so that you can identify that the issue you are troubleshooting is related to a problem of power supply. To find out more about tools that can be used to diagnose issues with power supplies, refer to Book 4, [Chapter 2](#).

**TABLE 6-2** Pin Configuration for the Main Power Connector

<i>Pin</i>	<i>Signal</i>	<i>Color</i>
1	+3.3VDC	Orange
2	+3.3VDC	Orange

<b><i>Pin</i></b>	<b><i>Signal</i></b>	<b><i>Color</i></b>
3	COM	Black
4	+5VDC	Red
5	COM	Black
6	+5VDC	Red
7	COM	Black
8	PWR_OK	Gray
9	+5VSB	Purple
10	+12V1DC	Yellow
11	+12V1DC	Yellow
12	+3.3VDC	Orange
13	+3.3VDC	Orange
14	-12VDC	Blue
15	COM	Black
16	PS_ON#	Green
17	COM	Black
18	COM	Black
19	COM	Black
20	Reserved	Varies
21	+5VDC	Red
22	+5VDC	Red
23	+5VDC	Red
24	COM	Black



**FOR THE  
EXAM**

The main power supply connector provides power at 3.3VDC, 5VDC, and 12VDC.

## *The floppy drive connector*

Although floppy drives are nearly obsolete, the floppy connector is an AMP 171822-4, four-pin connector; see its pin configuration in [Table 6-3](#). This connector provides power to a floppy drive at 5V but can supply power at either 5V or 12V to support devices from manufacturers that decide to use this connector. For compatibility, you will still often find one of these on your power supply.

**TABLE 6-3 Pin Configuration for the Floppy Power Connector**

<i>Pin</i>	<i>Signal</i>	<i>Color</i>
1	+5VDC	Red
2	COM	Black
3	COM	Black
4	+12V1DC	Yellow

### *The peripheral connector*

Until SATA drives rule the world, the four-pin peripheral connector is likely the most used power connector on most computers because it is used for hard drives (ATA/PATA) and optical drives. This connector is an AMP 1-480424-0 or Molex 8981-04P, and its pin configuration is shown in [Table 6-4](#). Like the floppy connector, it provides power at both 5V and 12V, but hard drives draw their power at 12V rather than the 5V sufficient for floppy drives. Hard drives require more power to get their heavier disk spinning.

**TABLE 6-4 Pin Configuration for the Peripheral Power Connector**

<i>Pin</i>	<i>Signal</i>	<i>Color</i>
1	+12VDC	Yellow
2	COM	Black
3	COM	Black
4	+5VDC	Red



---

## The 12-volt power connector

The 12-volt power connector (+12V2DC) — also called a *P4 connector* or *EPS connector* — is used to supply additional power directly to the processor. It uses a Molex 39-01-2040 connector; its pin configuration is listed in [Table 6-5](#).

**TABLE 6-5** Pin Configuration for the +12V2DC Power Connector

Pin	Signal	Color
1	COM	Black
2	COM	Black
3	+12V2DC	Yellow
4	+12V2DC	Yellow



**TIP**

You may also find the 8-pin (or dual 4-pin) versions of this connector on newer power supplies. They would have double the number of each pin type and use a Molex 39-01-2080 connector.

## The Serial ATA connector

The Serial ATA (SATA) drive offers two more connectors to the long list that are used by computers. One connector is used for data, and the other is used for power. The data connector is discussed in Book 3, [Chapter 1](#). The power connector uses a Molex 88751 connector, and an additional wire (5) supplies 3.3V to devices that require it. (Most functions of the SATA drive run on 12V.) The SATA connector has its five wires connected to 15 pins on the connector. The SATA connector pin configuration is listed in [Table 6-6](#).

**TABLE 6-6** Pin Configuration for the Serial ATA Power Connector

---

<b>Wire</b>	<b>Signal</b>	<b>Color</b>
1	+12VDC	Yellow
2	COM	Black
3	+5VDC	Red
4	COM	Black
5	+3.3VDC	Orange

## *The 6-pin PCIe connector and 8-pin PCIe connector*

The 6-pin PCI Express (PCIe) connector and 8-pin PCIe connectors are used to supply additional power to energy-hungry PCIe video cards. Many cards on the market contain either a 6-pin or 8-pin connector for this purpose. The only real difference between these connectors is the amount of power they can supply. The 6-pin connector supplies an additional 75W, and the 8-pin connector supplies an additional 150W. The 6-pin connector is listed in [Table 6-7](#), and the 8-pin connector is listed in [Table 6-8](#).

**[TABLE 6-7](#) 6-Pin Configuration for the Serial ATA Power Connector**

<b>Wire</b>	<b>Signal</b>	<b>Color</b>
1	+12VDC	Yellow
2	+12VDC	Yellow
3	+12VDC	Yellow
4	COM	Black
5	COM	Black
6	COM	Black

**[TABLE 6-8](#) 8-Pin Configuration for the Serial ATA Power Connector**

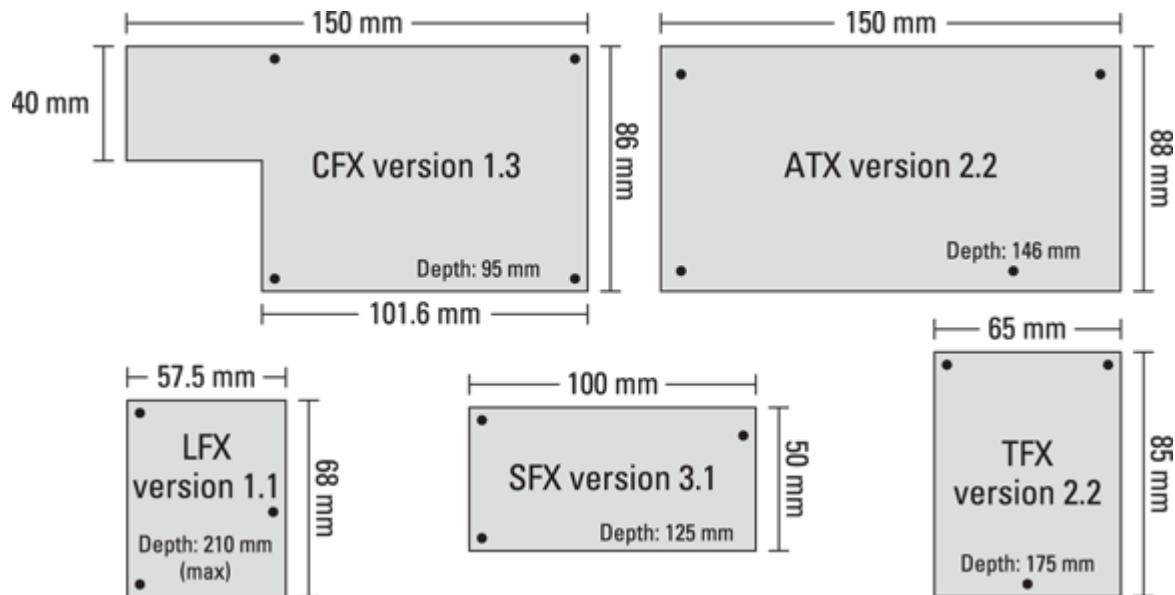
<b>Wire</b>	<b>Signal</b>	<b>Color</b>
1	+12VDC	Yellow
2	+12VDC	Yellow
3	+12VDC	Yellow
4	COM	Black
5	COM	Black
6	COM	Black
7	COM	Black
8	COM	Black

## ***Power Supply Form Factors***

In addition to the ATX form factors, there are many other power supply form factors that provide power for ATX motherboards. Different form factors exist mainly to fit in different sizes and styles of cases. These power supplies typically have the same types of power connectors that were detailed in the previous sections. The specifications for the power supplies usually define mounting points and the maximum footprint (space) that the power supply can occupy. In addition, the specifications also state whether cooling fans are required. In addition to the most common form factor — ATX v2.52 — form factors for the power supplies include the following:

- » **CFX v1.62** is the *compact form factor*, typically supplying power in the range of 220W to 300W.
- » **LFX v1.42** is the *low-profile form factor*, typically supplying power in the range of 180W to 260W.
- » **SFX v3.42** is the *small form factor*, typically supplying power in the range of 160W to 300W.
- » **TFX v2.52** is the *thin form factor*, typically supplying power in the range of 180W to 300W.

The size specifications for these, as well as the ATX power supply, are shown in [Figure 6-2](#). This figure also shows the mounting holes for each type of power supply. Computer power supplies are held in by three or four screws and are usually positioned in the top-rear portion of the computer. After removing the power connector from the internal devices, you can remove the screws and remove the power supply.



**FIGURE 6-2:** Power supply unit form factors.



**WARNING** Take care when removing the screws. Some cases have rails that support the power supply; with others, the power supply could drop onto the computer components in the case when the last screw is removed. Remember, you are only removing the mounting screws for the power supply, and not the screws to access the interior of the power supply. The power supply unit is a field replaceable unit (FSU), and you should not be attempting to service the interior of the unit, which is life-threatening.



TECHNICAL  
STUFF

Many mainstream servers from manufacturers such as IBM, HP, and others support multiple power supplies to provide redundant support in the event of a power supply failure. These power supplies have custom connectors on the server and are typically *hot-swappable* — allowing them to be replaced while the server is running. As a result, these power supplies have a variety of form factors that are not covered in this book.

## *Using AC Adapters*

Buildings run on alternating current (AC) and so do a variety of items that you connect directly to power outlets, including lamps and fans. Small electronics, such as your cellphone, do not require the amount power supplied by AC (120V or 240V) and are often designed to run on low voltage direct current (DC). The most common power source for DC devices is batteries. In order to connect a DC device to an AC power source, you need to convert or transform the AC power to the appropriate voltage DC power. The small block at the wall plug end of your cellphone charger makes this conversion for you.

Desktops have large internal power supplies to get AC building power converted to 3.3V, 5V, and 12V DC power for internal use, but laptops typically do not have the internal space to support such a large power supply. Most laptop AC adapters are external and have the job of converting the building power to a voltage that is required by the laptop. Laptops typically require between 12V and 20VDC. The laptop then has internal components that divide this incoming voltage into segments that are appropriated for the internal devices, such as 12V, 5V, and 3.3V. This allows for part of the power management components to exist outside the laptop.

In some cases, the power supply can use generic output voltages and connectors; in other cases, the voltage or connectors might be customized

by a manufacturer, meaning that replacement power supplies are tied specifically to that manufacturer.



TECHNICAL  
STUFF

AC adapters are used with a wide variety of devices that you deal with every day, converting AC power to DC power for smartphones, cordless phones, tablets, and a host of other devices. Always take care to match the correct power adapter to the power requirements for the devices to ensure that you don't damage the device — or worse.

When working with your AC adapter, always keep your eye out for possible damage along the length of the cord from wear or perhaps pets. Neat people actually tend to be harder on adapter cables than disorganized ones because neatniks tie up the cables every time they pack their laptops, consolidating the weight of the cable mass right next to the brick of the adapter, causing the cable to wear quickly in the section nearest the adapter. To avoid this problem, the cable should be coiled loosely and placed in your carrying case.

## WHAT ABOUT DC ADAPTERS?

*DC adapters* allow you to convert DC voltages to different DC voltages, changing the power characteristics, such as current, to allow 12V power from a vehicle to be used for computers and other equipment that do not use 12V power directly.

You may use these from time to time to power other devices. However, because the power requirements for most laptops are high, you might not be able to use a 12VDC adapter to provide it power.

If you need to use a high DC voltage device in a car, you will need to use a power inverter to convert the 12V DC car power back into 120V/240V AC power for use with your device.

## *Working with UPS and Suppressors*

Some people have such good and stable power that they take it for granted. This is not the reality for many of us, though, and we live with a

variety of power issues, such as these:

- » **Spikes:** Sharp increases in line voltage caused by a problem with the power utility equipment, which may be traced back to faulty transformers or lightning strikes.
- » **Power surges:** Similar to spikes, *power surges* are increases in line voltage that usually last longer than a spike.
- » **Noise:** Interference caused by items not directly connected to the power system. Power lines running near fluorescent lights or microwaves can have their AC sine waves altered or chopped, which affects devices receiving their power.
- » **Blackout:** A total interruption in the line power. The ATX power supply specification has a minimum voltage hold-up time of 17 milliseconds (ms), or about one-sixtieth of a second. This is how long the power supply can sustain computer operation during a power interruption. In other words, if your lights flick off and on because of a very short power outage, your computer might continue to run over that outage, but it would have to be a very brief power outage.
- » **Brownout:** The opposite of a power surge in that the line power is below normal for a period of time ranging from seconds to minutes. If the brownout exceeds the Input-Under Voltage limits of the power supply, the power supply will shut off.

Any of these input power supply situations may cause stress or damage to the devices receiving this type of power. Three basic devices help you deal with these power situations:

- » **Surge suppressors:** Protect your equipment against spikes and surges by quickly terminating the power connection before your equipment is damaged. These will not provide power when power is low, such as in cases of brownouts or blackouts.
- » **Line conditioners:** Take that a step further by cleaning the noise on the line and dealing with some under- and over-voltage situations, as well as generating alarms to notify you of any situations.

In most cases, line conditioners deal with surges and spikes while letting your equipment continue to function.

» **Uninterruptible power supplies (UPS):** Take power protection beyond line conditioners by keeping your equipment working even after total power failures. This is a battery backup for your computer systems.

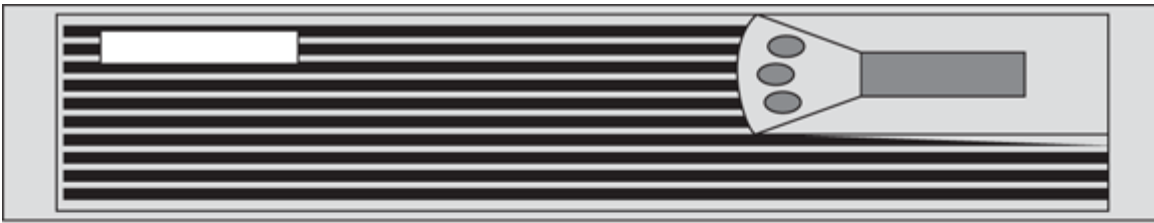
The two main types of UPSes are

- *Standby:* Also called *offline*, a standby UPS does not protect you from surges or spikes but takes over quickly in the event of voltage drops or failures. UPS units that are marketed toward home users are usually standby units.
- *Inline:* Also called *online*, an inline UPS always operates between the line and your equipment. In addition to providing power, when the UPS battery power is below a specific level, an inline UPS can initiate a graceful shutdown of the devices connected to it.

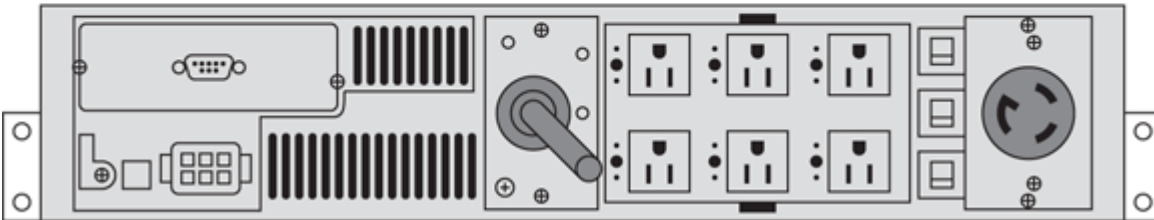
Most UPSes include scales or lights to indicate the current load on the UPS as a percentage of its maximum capacity, as well as the battery charge condition. Check these indicators regularly or install software that monitors the UPS for you. UPS indicators indicate capacity levels as well as error conditions.

UPSes often have a variety of options for receptacle types to supply devices with power. A standard server UPS is shown in [Figure 6-3](#). Notice the six 15-amp (NEMA 5-15R) receptacles as well as the single 20-amp twist-lock (NEMA L6-20R) receptacle. The 20-amp connector would be used to supply power to a Power Distribution Unit (PDU), which would likely have a series of standard 15-amp (IEC 320 C13) receptacles (NEMA 5-15R or IEC 320 C13; the IEC 320 C13 connector is what you find on the universal power cords used on most computing equipment).





UPS front view



UPS rear view

**FIGURE 6-3:** Front and rear of a standard server UPS.

Most UPSes are rated in volt-amps (VA), which indicates how much power they can supply. VA ranges for UPS start around 200VA and go up to tens of thousands of VA for corporate data centers.



TECHNICAL  
STUFF

In a perfect world, watts and VA would be identical. Early power supplies were capacitor input power supplies that used capacitors to even out the power supplied by a building's AC power. The method of converting power creates a variance between watts and VA of 55 percent to 75 percent, which is called the Power Factor (PF). This is represented by the formula

$$\text{watts} = \text{VA} * \text{PF}$$

Capacitor input power supplies are still in use on most inexpensive power supplies. The solution is the Power Factor Corrected (PFC) power supply, which uses watt and VA ratings that are the same. Most high-end equipment manufactured since 1996 should include a PFC power supply.

Before buying a UPS, total the power requirements for all the devices you want to plug into it, as well as the amount of time for which you need

protection. The protection time is usually between 10 and 20 minutes; longer protection periods are possible if you want to pay the additional cost. Use the information to make sure you get a UPS that is powerful enough to protect all your expensive gear. You will find tools to help perform these calculations on the website for most UPS manufacturers. The tool will allow you specify information about the devices you plan to connect and the protection time you require. With this information, the tool will make a product recommendation.

## *Getting an A+*

This chapter sheds light on power and how it interacts with your computer. The following points are covered:

- » The current specification of power supplies is ATX, and the ATX power supply will be found in one form factor or another on most current computers.
- » The main power connector has 20 or 24 pins. Four-pin floppy and peripheral connectors supply 5V and 12V, and five-pin SATA connectors supply 3.3V, 5V, and 12V.
- » Power supplies convert 120VAC or 240VAC power into DC power for the computer.
- » Power supplies come in a variety of power sizes, from 160W up to and beyond 1200W.
- » AC adapters are used on laptops to convert power from AC to DC, and usually automatically switch between 120V and 240V.
- » Surge suppressors, line conditioners, and UPS deal with various power-supply problems, including surges and brownouts.

## *Prep Test*

- 1. What are the main power voltages that are provided by standard computer power supplies? (Select all that apply.)**

- (A) 2.1V
  - (B) 3.3V
  - (C) 5V
  - (D) 12V
- 2. The local city power supply for your building has degraded to a point where you regularly suffer from blackout conditions. What device will help you deal with this issue?**
- (A) Capacitor
  - (B) Surge suppressor
  - (C) Inline UPS
  - (D) Line conditioner
- 3. What items should be considered when purchasing a UPS? (Select two items.)**
- (A) Power consumption of protected devices
  - (B) Types of hard drives in protected devices
  - (C) Runtime of protected devices
  - (D) Amount of RAM in protected devices
- 4. What are the standard input voltages for power supplies? (Select all that apply.)**
- (A) 110VDC
  - (B) 120VAC
  - (C) 240VDC
  - (D) 240VAC

## ***Answers***

1. **B, C, D.** ATX-based power supplies provide power to devices at 3.3VDC, 5VDC, and 12VDC. See “[\*Identifying the Purpose of Power\*](#)”

[Supply Units.](#)”

2. **C.** Inline UPS devices deal with blackout situations, while line conditioners may be able to deal with some brownout situations. Surge suppressors only deal with power surges, while capacitors are electronic devices which can store an electrical charge. Review [“Working with UPS and Suppressors.”](#)
3. **A, C.** Both the desired runtime of devices, as well as their power consumption, are required to determine the required performance characteristics of a UPS, as they will determine the size of the required battery capacity in the UPS. Check out [“Working with UPS and Suppressors.”](#)
4. **B, D.** 120VAC and 240VAC are the two power input voltages that are handled by power supplies. Peruse [“Identifying the Purpose of Power Supply Units.”](#)

# Book 3

## Outside the Box

### Contents at a Glance

#### Chapter 1: Identifying Basic Cables and Connectors

[Video Cables](#)

[Audio Cables and Connectors](#)

[Multipurpose Cables](#)

[Serial Cables](#)

[Hard Drive Cables](#)

[Adapters](#)

[Getting an A+](#)

[Prep Test](#)

[Answers](#)

#### Chapter 2: Installing and Configuring Input Devices

[Minding Your Keys and Qs](#)

[Catching the Mouse](#)

[Communicating with Network Adapters](#)

[Other Input Devices](#)

[Getting an A+](#)

[Prep Test](#)

[Answers](#)

#### Chapter 3: Installing and Configuring Output Devices

[Understanding Video Adapters](#)

[Using Your Monitor or Display](#)

[Troubleshooting Display Issues](#)

[The Sound of Computers](#)

[Other Output Devices](#)

[Getting an A+](#)

[Prep Test](#)

[Answers](#)

## **Chapter 4: Managing Printers**

[Learning about Paper Feeder Mechanisms](#)

[Understanding Types of Printers](#)

[Viewing Types of Printer Connections and Configurations](#)

[Upgrading Printer Hardware](#)

[Installing a Printer in Windows](#)

[Troubleshooting Printer Problems](#)

[Understanding Safety and Preventive Maintenance](#)

[Getting an A+](#)

[Prep Test](#)

[Answers](#)

## **Chapter 5: Working with Multimedia Devices**

[Understanding Scanners](#)

[Using Digital and Web Cameras](#)

[Looking at Other Multimedia Devices](#)

[Getting an A+](#)

[Prep Test](#)

[Answers](#)

## **Chapter 6: Dealing with Laptops and Mobile Devices**

[Identifying Portable Computer Components](#)

[Looking at Laptop Batteries](#)

[Understanding AC Adapters](#)

[Learning about LCD Panels](#)

[Understanding Laptop Input Devices](#)

[Laptop Communication Components](#)

[Port Replicators and Docking Stations](#)

[Expanding on a Laptop](#)

[Upgrading Your Laptop](#)

[Mobile Operating System Types](#)

[Troubleshooting Laptop Issues](#)

[Disassembling and Reassembling Laptops](#)

[Understanding Smartphones/Converged Devices](#)

[Securing Mobile Devices](#)

[Getting an A+](#)

[Prep Test](#)

[Answers](#)

# Chapter 1

## Identifying Basic Cables and Connectors

---

### IN THIS CHAPTER

- » Reviewing basic cable types, features, and their purposes
  - » Identifying common connector types
- 

In this chapter, you examine the ports on the back of the computer as well as the cables and connectors used to attach devices. Other chapters of this book examine the different devices, but this chapter looks at getting them all connected. The other devices and chapters include

- » **Printers:** Book 3, [Chapter 4](#)
- » **Internal drives:** Book 2, [Chapter 5](#)
- » **Monitors:** Book 3, [Chapter 3](#)
- » **USB devices:** Book 2, [Chapter 1](#)

A CompTIA A+ Certified Professional must be able to identify various types of cables and connectors. This chapter introduces you to the most common cables and connectors that you will encounter when using computer systems.

Start by looking at the different types of ports on the back of your computer. *Ports* are connection points on your computer that allow for devices to be connected to your computer. The connection point has a connector that accepts a cable with a matching connector. Knowing what the ports are used for is important when connecting devices to your computer. You might already be familiar with some of the common ports, such as video and USB (Universal Serial Bus).



In the sections that follow, you examine several different types of cables and discover the uses of each type. Some of the cables are used inside your computer, and others are external. After you complete this chapter, you should be able to identify the basic types of cables and where they are used. In addition to examining the types of cables you would use for various roles, you also examine the connectors that exist on each of those cables.

## *Video Cables*

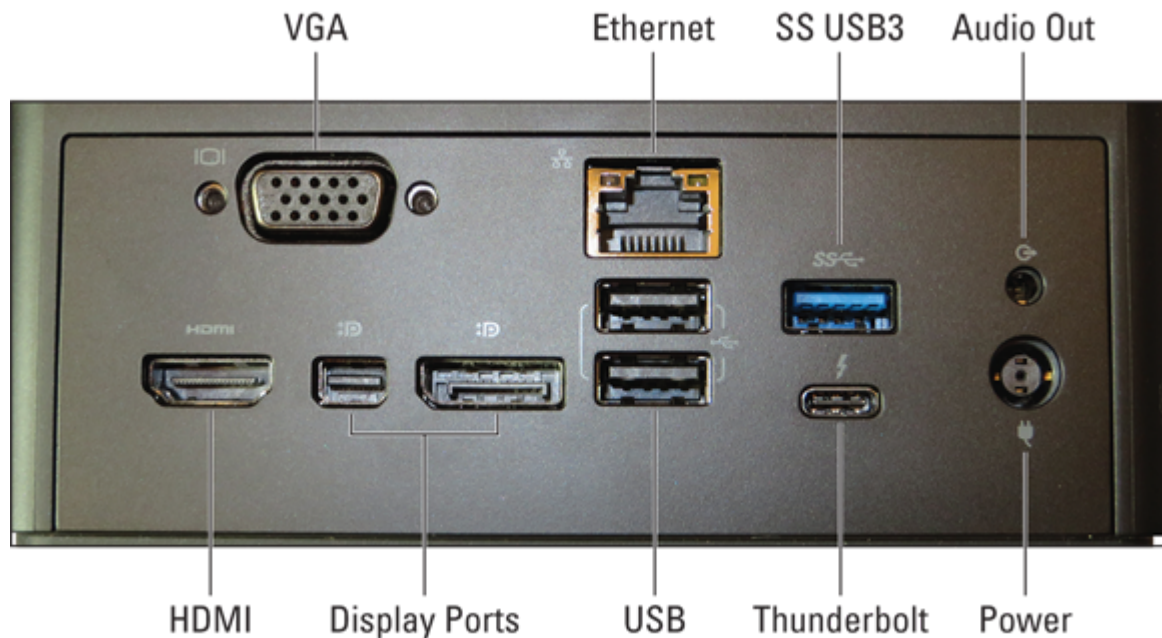
You need to see what you're doing, so the monitor connection plays an important role. The latest generation of video devices typically include either HDMI or DisplayPort connections in one of the connector's standard sizes. You can expect to see full-sized ports on desktop computers, and mini versions on laptops and mobile devices. The drive in the video industry over time has been to drive more colors at a higher resolution and at a higher frequency, giving you a better image quality. This section looks at the different options you have related to video connections to your computer.

### *VGA*

With the demise of the MDA (Monochrome Display Adapter), HGC (Hercules Graphics Card), CGA (Color Graphics Adapter), and EGA (Enhanced Graphics Adapter) monitor types as well as the release of VGA (Video Graphics Array), SVGA (Super Video Graphics Array), and XGA (Extended Graphics Array) monitors, the monitor connector on the back of your computer changed from a DB-9 female connector to an HD (high density) DB-15 female connector also known as DE-15. While people often refer to this connector on their computer as a VGA connector, the circuitry and video support is likely SVGA or XGA.

The connector for this video standard was a D-shell connector, since it is thought to resemble a capital D. This connector was the same size as the DB-9, but had 15 pins instead of 9. DB-15, also known as HD DB-15 or HD-15, has the familiar shape of the D-shell connector that contains a high density (HD) pin arrangement, with three rows of five connection

points rather than the traditional two rows. For VGA and SVGA monitor connections, look for this connector in its female form on your monitor and computer, which will be connected with a cable containing two male connectors. [Figure 1-1](#) shows the DB-15 connector on the back of a docking station.



**FIGURE 1-1:** A docking station with a variety of video interfaces.

## *HDMI and Mini-HDMI*

The home video market has standardized the HDMI (High-Definition Multimedia Interface) video connector type and video signaling standard. HDMI is a proprietary standard for audio and video transmission. This connector has made its way into the technology arena and can also be found on computers and monitors.

Like most standards in technology, HDMI has gone through many evolutions from HDMI 1.0, which was similar to DVI and allows for 4.95 Gbps of data transmission, to HDMI 2.1, which allows for up to 48 Gbps of data transmission. HDMI 2.1 is capable of supporting high-resolution displays at 8K and higher resolutions, which is a great increase over the original 720p and 1080p resolutions.

This 19-pin connector is capable of providing both video and audio signals, and has been adopted by the computer industry for both multimedia and nonmultimedia computers, giving people a wider variety of output devices. HDMI uses the same video signaling as DVI, which makes it compatible with computer displays while providing superior performance characteristics when compared to VGA. Also, remember that VGA is analog, while HDMI is digital.

You can see an HDMI port back in [Figure 1-1](#). The full-sized port appears on larger devices such as desktop computers and some laptops, while the small Mini-HDMI connector is found on smaller devices like laptops and tablets. This smaller connector has 19 pins as well, and the same basic shape of the full-sized connector, but is about half the height and width. For even smaller device connections, there is also a Micro-HDMI connector.

### ***DisplayPort and Mini-DisplayPort***

Like HDMI, DisplayPort was created as an alternative digital video port to replace the aging analog VGA interface. It was created to not only carry video, but also audio and other data, such as USB data. Unlike HDMI, DisplayPort did not seem to gain a foothold in the home entertainment market, and is now focused on the technology market. Both HDMI and DisplayPort took aim at the DVI interface.

As with HDMI, DisplayPort has not been stationary since it was created, and its specification went from 1.0 to 1.4. The DisplayPort 1.0 specification allowed for 10.8 Gbps of bandwidth, while DisplayPort 1.4 supports 32.4 Gbps and new 4K and 8K displays.

Similar to HDMI, there are a few different sizes of the 20-pin DisplayPort and Mini-DisplayPort, which looks like a rectangle with one corner cut off. You can see examples of both of these ports in [Figure 1-1](#). Notice that the two DisplayPort icons have two + symbols, identifying them as Dual Mode DisplayPort. Even without this icon, most DisplayPorts are Dual Mode.

Dual Mode DisplayPorts detect the device at the other end of cable and if it is HDMI or DVI, they will send DVI/HDMI signals instead of the

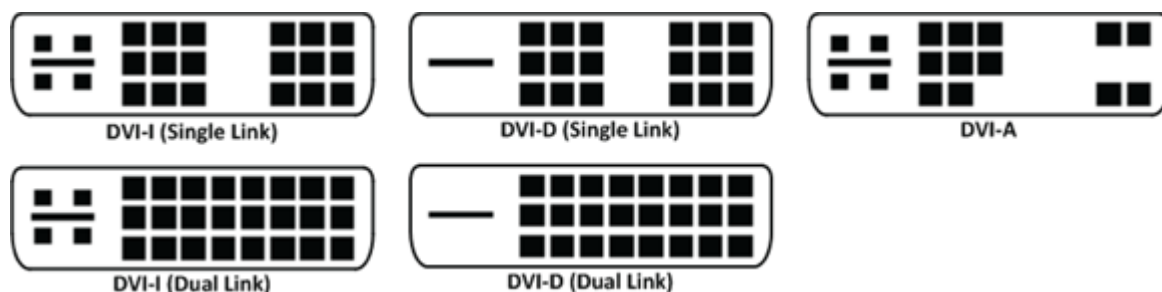
standard DisplayPort signals. Dual Mode allows for the use of a passive adapter to convert the cable over to DVI/HDMI on the receiving end.

## ***DVI***

With the universal adoption of LCD/LED monitors, a higher-definition port was adopted for computer and video cards to support the higher throughput and digital signals LCD monitors require. This port is a DVI (Digital Visual Interface) port and accepts a monitor connector that has as many as 24 digital pins and optionally 5 analog pins (for backward compatibility).

If you have been working with DVI connectors for a while, you may have noticed that they are not all the same. [Figure 1-2](#) shows the main variants of DVI connectors, while their uses include the following:

- » **DVI-I (single link and dual link):** The *I* in the name is for *integrated*, as this port type supports digital and analog video signals over the same connection, allowing either type of monitor to be connected. Dual-link connectors send twice the video signal, allowing them to be used on large high-performance displays or over a longer distance. Analog signal support is provided by the four pins on the left of the connector and needs an adapter to support the standard 15-pin VGA connection. This is the standard used for monitors that have DVI, which is most monitors.
- » **DVI-D (single link and dual link):** The *D* in the name is for *digital*, as this port type supports only digital video signals. Again, this port type has single-link and dual-link variations.
- » **DVI-A:** The *A* in the name is for *analog*, as this port type supports only analog video signals and is used for connections to analog monitors through an adaptor.



**FIGURE 1-2:** DVI connector variants.

When looking at digital video solutions, there are a few additional facts you should be aware of:

- » HDMI and DisplayPort connections support sending audio signals over the connection, in addition to digital video signals.
- » HDMI and DisplayPort support only digital signals, while DVI has backward support for analog signals.
- » DisplayPort is a new royalty-free digital video standard. While it is not compatible with DVI or HDMI, the newer DisplayPort++ ports can be used with an external adapter to provide video signals to DVI and HDMI devices. Analog signals cannot be provided without an external converter.
- » DisplayPorts are similar in dimensions to HDMI, making them less than half the size of VGA or DVI ports, and very useful on mobile devices.
- » HDMI and DisplayPort both have smaller port designs, which are used on tablets and other small electronics; HDMI standards are supported on mini-HDMI, while DisplayPort standards are supported on mDP (mini DisplayPort).

You can read more about connecting monitors to your computer in Book 3, [Chapter 3](#).

## *Audio Cables and Connectors*

Several standard types of connections are used for audio purposes. [Table 1-1](#) lists two standard audio connectors and their uses. Analog audio purists may laud the slow or continuous change in tones from an analog sound system, resembling the smooth sine wave. But for computers that process everything in harsh 0s and 1s, the squared of digital signal is easier and faster to process. If you can avoid the translation between analog and digital signals, you should.

**TABLE 1-1** Types of Multimedia Connectors

Role	Connectors Used
Analog audio	The main analog audio connector used in your computer is the one-eighth-inch connector or 3.5 mm connector, which is the standard headphone, speaker, and microphone jack for most sound cards. This form of connector has been around for years as an audio connector.
Digital audio	The main digital audio connection for your computer is a S/PDIF (Sony/Philips Digital Interface Format) connection. Many motherboards and soundcards support this interface for multimedia applications. The S/PDIF connection is often made using coaxial, RCA, or optical connectors and cables.

## *Multipurpose Cables*

In addition to the dedicated cable types for video and audio data transfers, certain other cable types are used for a multiple of purposes, such as Ethernet connections and connecting drives, phones, and printers.

### *Lightning*

The Lightning connector is a proprietary Apple connector and is designed to work with Apple products, most notably Apple phones and tablets. The connector is an 8-pin connector designed to be used in either orientation, as opposed to single-orientation connectors like HDMI and DisplayPort connectors.

While the Lightning cable is typically a USB 2.0 cable, the port is supported on USB 3.0 as well, and this cable can be used for data transfer and charging. The port on the device is able to use the Lightning

connection for other purposes, such as providing audio output, since the latest generation of Apple phones no longer have 3.5-mm audio jack.

## ***Thunderbolt***

The original Thunderbolt interface was developed by Intel and embraced by Apple in its devices. Thunderbolt is a high-speed databus capable of multiplexing multiple signals over a single cable and provides access to the PCIe databus as its main interface.

Thunderbolt 1.0 supported 2 10 Gbps channels, providing 20 Gbps of data transmission, and support for up to 6 Thunderbolt devices; Thunderbolt 3.0 supports 40 Gbps of transmission. Thunderbolt 1.0 and 2.0 made use of the 20-pin Mini-DisplayPort connectors, while Thunderbolt 3.0 now makes use of the 24-pin USB-C connector. Since data channels are multiplexed, and since early Thunderbolt was making use of the DisplayPort connector, in addition to the PCIe data, it also supports DisplayPort data and signals over the single connection. Similarly, since Thunderbolt 3.0 is making use of the USB-C connector, it supports PCIe data channels, as well as DisplayPort data and USB 3.1 data, making it a flexible, all-in-one port. You can identify Thunderbolt ports and cables by the bolt of lightning symbol, as shown in [Figure 1-3](#).



**FIGURE 1-3:** Thunderbolt USB-C connectors. Note the Thunderbolt icon on the left connector.

When connecting a Thunderbolt device to a Thunderbolt port on a computer, the Thunderbolt circuitry will be activated. If you connect a USB device to a port, it will only use the USB circuitry.

Power over the Thunderbolt connector is also impressive, making it an ideal solution for docking stations and requiring a single cable to your computer. From a docking station, the Thunderbolt connector can supply up to 100W of power to your laptop, eliminating the need for a power adapter on the laptop when connected to the dock, but this is based on the power requirements of your laptop. In addition to this power, it is able to supply up to 15W of power to bus-connected devices, making it a much more “powerful” bus technology than USB.



## USB

USB (Universal Serial Bus) is a more modern method of communicating using serial communication methodologies. The standards for USB 1.0 were released in 1996, USB 1.1 in 1998, USB 2.0 in 2000, USB 3.0 in 2008, and USB 3.2 in 2017. The goal of USB was to revolutionize how serial communication was conducted. To fulfill this goal, USB uses a cabling system that allows up to 127 devices to be connected. It also delivers power to the devices connected on this bus.

To go along with this new cabling, the specification for USB dictates that all devices should support Plug and Play. With these two pieces of the puzzle put together, USB enables you to plug in devices and have them work without having to worry about power cables or drivers. Some USB devices that require a large amount of power may use a supplemental power supply, but the USB bus will power most devices.

USB 2.0 increased the fastest transfer rate for USB 1.0 from 12 Mbps to 480 Mbps. This has allowed it to be used for devices that require faster transfer rates, such as hard drives and CD-ROMs. USB 3.0 takes that a step further, allowing for device communication up to 5.0 Gbps (also called Super Speed), while USB 3.1 doubled that, and USB 3.2 doubles that again by supporting 20 Gbps over the USB-C connector.



FOR THE  
EXAM

USB has had a performance boost up to 480 Mbps with the introduction of version 2 of the USB standard. For the A+ exams, you need to pay attention to the version of USB covered in the question. If it is USB 1.0, you are still limited to the 12 Mbps transfer rate, while USB 2.0 is 480 Mbps, USB 3.0 is 5.0 Gbps, USB 3.1 is 10 Gbps, and USB 3.2 is 20 Gbps.

USB 1.0, USB 2.0, and USB 3.0 all use proprietary connectors (shown in [Figure 1-4](#)) to connect as many as 127 devices. All these devices must be *hot swappable* (capable of being added or removed without turning off the computer), thanks to the specification for the standard. These connectors represent the most common connectors used with USB:

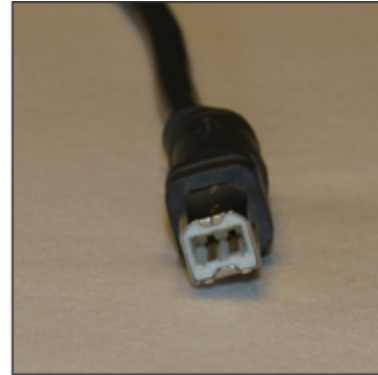
- » Type-A connectors are used to connect to ports on your computer.
- » Type-B connectors are used to connect to ports on your devices, such as printers or hard drive enclosures.



Type-A



USB 3.0 Type-A



Type-B



Mini-B



Micro-B



USB 3.0 Micro-B

**FIGURE 1-4:** A sample of the most common USB connectors.

With the advent of smaller and smaller USB devices, the device end of the cable has many smaller cousins, such as the mini-A, mini-B, micro-A, and micro-B connectors. The original USB connector is a 4-pin connector, while the mini and micro connectors are 5 pin connectors following the USB 2.0 standard. Both mini and micro connectors have similar form factors that make getting your cables confused very easy. These connectors are found on many MP3 players, digital cameras, and cellphones.

USB 3.0 achieves its performance increase by using more wires in the cable to pass additional data, and this connector uses 9-pins. If you look

closely at the USB 3.0 Type-A connector, you can see a second set of pins or contacts farther back in the connector. This allows connections to USB 3.0 ports on your computer to make use of the additional connections, while USB 2.0 ports will only make contact with the front contacts. This makes the connector backward compatible with USB 2.0 ports, without needing to carry around two sets of cables. On the device side, the USB 3.0 Micro-B connector has two sections, one that resembles a Micro-B connector and then a portion that makes use of the extra wires in the cable. To make the USB 3.0 connectors and ports easy to spot, the USB 3.0 specification defines that the plastic guides on these connectors are to be blue.

USB 3.2 introduces a new connector, the USB-C or USB Type-C connector. This is the same connector which is used in the Thunderbolt 3.0 specification and can be seen back in [Figure 1-3](#). This is a 24-pin connector. To support full-feature USB 3.1 and USB 3.2 applications, you would use a cable with one of these USB-C connectors on each end of the cable, connecting a computer with a USB-C connector to a device with a USB-C connector.



TECHNICAL  
STUFF

USB performance has improved over the years, with USB 1.0 having a maximum speed of 12 Mbps and a maximum cable length of 5 meters (16.4 feet) when working with Full Speed devices; it was 1.5 Mbps and 3 meters (9.8 feet) for Low Speed devices. USB 2.0 raised the speed limit of devices to Hi Speed at a whopping 480 Mbps and a maximum cable length of 5 meters (16.4 feet). Finally, USB 3.2 has brought the speed limit up to Super Speed at 20 Gbps, and the cables have a practical limit of approximately 3 meters (9.8 feet).



TECHNICAL  
STUFF

By bringing the speed of USB up to 5 Gbps in USB 3.0 devices, a second option now exists for people who want to achieve maximum throughput for external hard drives. Prior to USB 3.0, eSATA was the preferred method for high-speed external drives.

Power may also be provided over the USB interface, with USB 1.0 and USB 2.0 providing up to 500mA, USB 3.0 providing up to 900mA, and USB 3.2 providing up to 3 A. Standard USB controllers and ports are limited to only providing 100mA of power until the device requests more current, while some laptops and other devices have a charging port that will provide the maximum amount of power when a device is connected. This port is useful for supplying power to nonintelligent devices.

USB allows for support for up to 127 devices, and you will not likely have that many ports on your computer to plug them all in. The solution to this problem is the USB hub. USB hubs support two modes: passive and active. A *passive* hub is just that, passive. It allows for the wire-based connections between all the ports, which allows all the devices to communicate. The passive hub does not add any extra power to bus, so if you have several high-power devices, such as disk drives, you will find that you do not have enough power for all the devices. *Active* hubs, on the other hand, support the USB bus by helping to keep the signal strong and enable the management of circuits that require power. The power used by active hubs is also used to power the higher-power devices, such as USB hard drives.

## *Serial Cables*

Older computers have one or two serial ports, and you will still find serial ports on special-purpose computers, such as production control devices in factories. This port is used to connect devices, such as modems and control systems, to your computer. I still work with many older network devices where a direct console connection for administration is done via a serial port. And if my computer does not have a serial port, I

need to resort to a USB to Serial adaptor, which often has varying degrees of success. So while for the mainstream population, serial is a dead connection, for some of us they will still be in use as long as these legacy devices exist in the world.



TECHNICAL  
STUFF

There has been a trend in the industry to create legacy-free computers: that is, computers without COM ports (serial ports), LPT ports (parallel ports), or ISA expansion slots, as well as number of other functional changes. All but a few machines in market fit into this category.

*Parallel ports* send data over multiple wires simultaneously; *serial ports* send data over only one wire at a time. Parallel communication allows for multiple streams of data, which in the early days, when serial controllers were slow, allowed it to provide higher data transfer rates than serial communication. This is no longer true today.

Serial ports, on the other hand, deliver data sequentially down a single wire. Eight bits of digital data are converted into an analog signal by using a system called baud. *Baud rate* refers to the number of state changes (tones) made on the wire in any given second. If you have heard a fax machine or modem making a connection, you have heard the state changes as a series of squeals. Baud rate is very different from bits per second (bps), which measures the amount of data that is transferred. At one point, 300 bps modems communicated at 300 baud, but compression standards adopted by the communications industry allowed more data to be delivered at the same baud rate. This means that a 56 Kbps (57,344 bps) modem communicates at 9,600 baud.

Depending on the baud rate used to transfer data, the length of the cable can range up to 3,000 feet (just over 900 meters). For data transfer rates at 9,600 baud, the maximum cabling length is 250 feet (just over 75 meters). The RS-232C standard (usually simply referred to as RS-232), which is used as a basis of serial communication, recommends a maximum cable length of 50 feet (about 15 meters).

When working with cables and connectors, there are pins and holes on the connector, which are used to connect wires in the cable. With USB and other cables, you hardly see the contacts on the connector, but with the older serial cable, the pins are very obvious. The pins on the connectors are numbered, which is important to know when looking at the next section.

Looking at the connector with the D pointing toward the ground, pin numbering on male connectors starts with the top-left connector. With the connector in this orientation, the upper-left pin is pin 1, and the order goes across the connector and left to right for all subsequent rows. For a female receptor, hole 1 or pin 1 is in the top-right of the connector if the D is pointing down; other pins are numbered right to left. This allows pin 1 on a male connector to match pin 1 on a female connector. This section covers the two most common serial cables.

### *Standard serial cable*

This cable is used to connect a COM port on your computer to a modem or other device that could be used for Out of Band Management. This cable can easily be confused with custom communications cables, but verifying the pin configuration with a multimeter or continuity tester will ensure you have the correct cable. Numbering the pins on the connectors makes it easier to describe what the cable looks like at the connector level. This might make more sense when you look at the pin configuration for a standard 9-pin to 25-pin serial modem cable, and the 9-pin to 9-pin null modem cable in the next section. Modem cables are designed for a computer with either a male 9-pin connector or a male 25-pin connector, so the cable has either a female 9-pin or a female 25-pin connector on the end that connects to the computer, and a 25-pin male connector on the end that connects to the modem. Older computers have a 9-pin serial connector. The pin configuration and function for a 9-pin to 25-pin serial cable are summarized in [Table 1-2](#).

**TABLE 1-2 Serial Cable Pin Connections**

<i>Computer (9-pin)</i>	<i>Data Direction</i>	<i>Modem (25-pin)</i>	<i>Role</i>

<b>Computer (9-pin)</b>	<b>Data Direction</b>	<b>Modem (25-pin)</b>	<b>Role</b>
3	→	2	Transmitted Data (TD)
2	←	3	Received Data (RD)
7	→	4	Ready To Send (RTS)
8	←	5	Clear To Send (CTS)
6	→	6	Data Set Ready (DSR)
1	→	8	Data Carrier Detected, or tone from a modem (DCD)
4	→	20	Data Terminal Ready (DTR)
5	N/A	7	Signal Ground (SG)
9	←	22	Ring Indicator, or ringing tone detected (RI)

## *Null modem cable*

If you need to transfer data via serial ports between two computers that are close, use the same communications programs as if you were actually using modems and telephone lines to connect the computers. Such serial communication (that bypasses a modem) uses a *null modem cable*, which nullifies or eliminates the need for a modem by directly connecting the send and receive ports of the devices on either side of the cable. [Table 1-3](#) shows how the pin connections are made between devices. If you look at the roles of the pins on each side of the connection, you can see that each pin that sends data is connected to the receive pin for that data on the other side of the cable, with the result that a transmit data pin is connected to a receive data pin.

**TABLE 1-3 Null Modem Cable Pin Connections**

<b>Role</b>	<b>Computer (9-pin)</b>	<b>Data Direction</b>	<b>Computer (9-pin)</b>	<b>Role</b>
RD	2	→	3	TD
TD	3	←	2	RD
RTS	7	→	8	CTS
CTS	8	←	7	RTS

<i><b>Role</b></i>	<i><b>Computer (9-pin)</b></i>	<i><b>Data Direction</b></i>	<i><b>Computer (9-pin)</b></i>	<i><b>Role</b></i>
DCD and DSR	1 and 6	←	4	DTR
DTR	4	→	1 and 6	DCD and DSR
SG	5	N/A	5	SG



**TECHNICAL  
STUFF**

If you work with a computer networking group, you will find that null modem cables are still very popular, as many network devices still require an initial setup of configuration changes that are performed via a serial port on the device. This is true for switches and routers, where the serial port is called a console port and is connected to your computer by using a null modem cable.

## ***Serial connectors***

The following sections look at the two most common types of serial connectors you will encounter.

### ***DB-9 connector***

The DB-9 connector is a D-shell–type connector, so named because of its D shape. The DB-9 has nine connection points arranged in two rows. This connector used to be found on the back of a computer in its female form, to be used with a CGA or EGA monitor. Now, you’ll find a male DB-9 connector on the back of a computer as one of the two types of serial connections for COM ports. [Figure 1-5](#) shows female and male DB-9 connectors.





**FIGURE 1-5:** The DB-9 connector.



TECHNICAL  
STUFF

While COM ports have fallen out of the mainstream due to faster and easier connectivity options, such as USB, you will still see COM ports on computers used for some Out of Band Management solutions and for device configuration for many devices found in your data center. These devices include items such as routers, switches, and controller or management cards.

### ***DB-25 connector***

Once again, you see the familiar shape of the D-shell connector on a DB-25, but this connector sports 25 connections arranged in two rows. This connector is found on your very old computer in its male form in the role of a serial port and in its female form as a parallel port. You can also find the 25-pin male connector on the back of most modems. [Figure 1-6](#) shows a parallel cable and a serial 9-25 pin converter; the latter is used to convert a 25-pin serial connector on the back of a computer down to a 9-pin port to be compatible with a 9-pin serial cable.



**FIGURE 1-6:** The DB-25 connector.



**TIP**

If you find yourself routing around an old box of cables looking for a serial cable, keep in mind that not every cable with a DB-25 connector is a serial cable, as it could be a parallel extension cable, which will have a male BD-25 connector to attach to your computer and a female DB-25 connector to attach to a parallel printer cable. This cable can easily be confused with a serial cable for a computer with a 25-pin serial connector. The only way to positively identify this cable is to use a multimeter or a continuity tester to see what pins on one end of the cable match which holes on the other end. For a parallel extension cable, this is a straight-through cable; and, each pin, 1 through 25, matches with the appropriate hole on the other end of the cable.

## *Hard Drive Cables*

Hard drives have been around for almost as long as computers have, in a relative perspective, and during that time they have changed in physical size, storage capacity, speed, and more recently, storage format. Even with all these changes, the attachment mechanism has not changed nearly

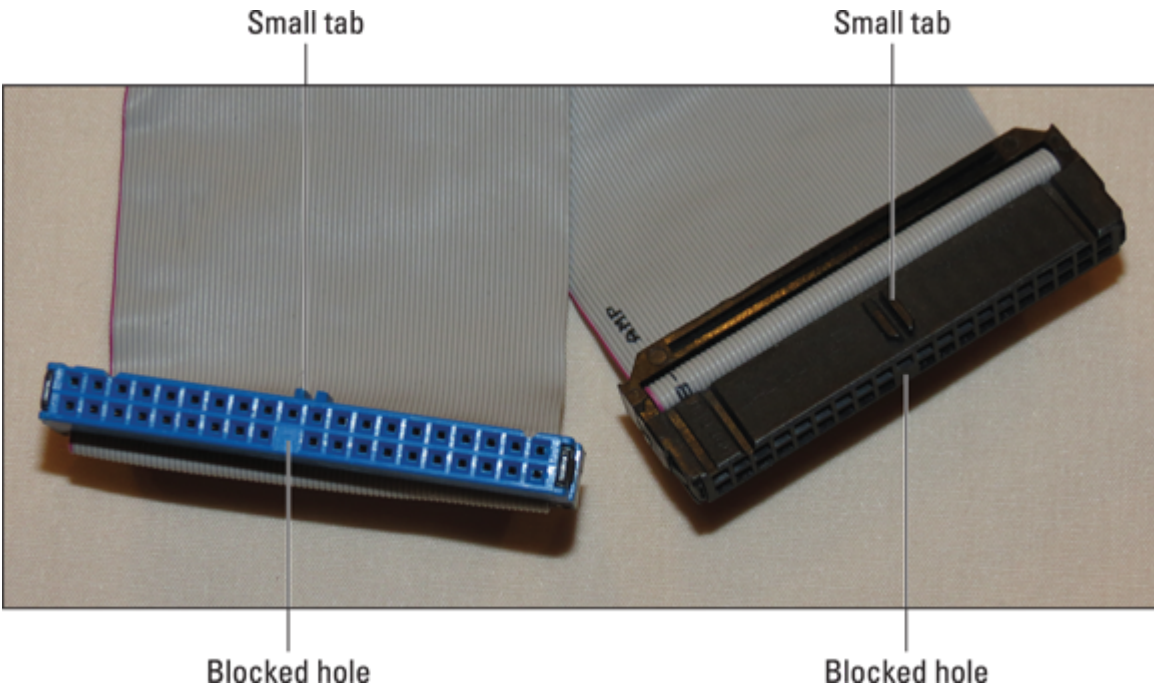
as fast. This section takes a look at those attachment or connection mechanisms.

You can read more on the topic of drives in Book 2, [Chapter 5](#).

## ***IDE***

For desktop computers, the IDE (Integrated Drive Electronics) interface is the oldest interface still in active use. First used in the 1980s, this standard has since been renamed to ATA (Advanced Technology Attachment), and when compared to other ATA standards, is specifically referred to as PATA (Parallel ATA).

The ATA connector is strictly an internal connector based on a 40-pin connector and a ribbon cable, which is shown in [Figure 1-7](#). While the first connectors were easily connected incorrectly, newer forms of the connectors are keyed to prevent accidental installation. (Note the tab and the blocked hole on the connector in [Figure 1-7](#).) As with the serial connector, the holes and pins on this connector are numbered from 1 to 40. The pins are typically found on your motherboard or hard drive, and there will be an indicator to show you where pin 1 is located. For the ribbon cable, pin 1 is identified with a different color wire — typically red or blue. The only way for the cable to be plugged into the connector is if the tab on the cable matches the notch on your device, and there is only one way for that to happen — pin 1 must be lined up on your connectors.



**FIGURE 1-7:** Ribbon cable used for IDE/ATA connections.



**TIP**

The connector with the pins is the *male* connector, and the connector with the holes is the *female* connector. And even though the female connector does not have pins, the holes on the female connector are typically referred to as pins.

The IDE interface has been improved over the years, going from IDE, to EIDE (Enhanced IDE), to UDMA (Ultra Dynamic Memory Access), to Ultra ATA, and to Ultra ATA/133. If you see any of these terms when working with your computers, they are all forms of PATA, and you will see them used interchangeably.

As the speeds increased toward the current 133 MBps, we saw a change in the ribbon cable used for IDE, which went from a 40-wire ribbon cable to an 80-wire ribbon cable, with every second wire being used as ground to prevent cross-talk between the data wires. As the name implies, Parallel ATA sends data down the wire in parallel while serial communication would send one block of data down the wire at a time.

The IDE interface and cables allow for up to two devices to be connected to a single port, while hard drives would have two connectors, one 40-pin connector for the IDE/ATA cable, and one Molex 8981-04P 12V power connector.

You can read more about power connectors in Book 2, [Chapter 6](#).

## **SATA**

SATA (Serial ATA) is the newer hard drive attachment interface and was first released in 2003. The first version of the SATA standard supported transfer speeds of 150 MBps and was referred to SATA-150, while SATA 3.0 brought this up to 600 MBps in the form of SATA-600. The most current revision of SATA 3.0, SATA 3.2 brings the speed up to 1969 MBps and is used by new SATA M.2 drives to offer extreme disk performance.

As ribbon cables, PATA cables often caused issues with cooling when used in smaller computer chassis. As part of the SATA design, the cables were much smaller and had a lower impact on internal cooling of computer chassis. When it comes to the connectors, regardless of the SATA standard, the connector has remained the same, with some exceptions with the latest drives. Outside of mSATA (Mini-SATA) and SATA M.2 connectors, the connector on all SATA drives and cables have remained the same. For external SATA drives, you will also find external SATA (eSATA) connectors. Although the external side of the eSATA connector is keyed differently, it still has the same number and order to its pins. You can see both the eSATA and SATA connectors in [Figure 1-8](#).



**FIGURE 1-8:** SATA and eSATA connectors.

When connecting external drives, eSATA offers advantages of other connection interfaces, such as USB 2.0, since the drive was connected directly to the internal SATA bus through an external connector. This connection provided an improved speed and removed a layer of translation between the drive and the USB bus.

You can read more on the topic of drives in Book 2, [Chapter 5](#).

## ***SCSI***

SCSI (Small Computer System Interface) is a standard for connecting peripherals to your computer, and is most often used to attach hard drives and tape drives to computers. SCSI has been a standard for server hard

drives, but in the desktop arena it was only used on MacIntosh computers, but Apple has since switched over to using PATA and SATA drives.

The original SCSI standard was parallel and allowed for 5 MBps transfer rates, increasing over years to 320 MBps. This standard made use of internal ribbon cables with 50, 68, or 80 pins, while externally they make use of Centronics-style connectors. You can see what SCSI connectors look like in Book 2, [Chapter 5](#) in [Figures 5-14](#) and [5-15](#).

The SCSI standard continue to be used for servers with RAID arrays, and eventually grew to make use FC (Fiber Channel) interfaces, with supported transfer speeds from 1 Gbps to 14 GBps. In addition to FC drives, the standard moved to SAS (Serial Attached SCSI) which grew from supporting transfer speeds of 3 Gbps to 22.5 Gbps in the SAS 4.0 standard.

## *Adapters*

With the similarity between bus standards and the flexibility of expansion ports like USB, you can transfer the role of one port into many other functions. Keep in mind that some adapters may be passive when the signal on the wire is compatible with the port and device type, but if the signal needs to be converted, the adapter needs to be powered and have circuitry to convert the signal. In many cases, the power can be provided by the port itself. Here are some examples of the conversions that can be accomplished:

- » DVI to HDMI
- » USB A to USB B
- » USB to Ethernet
- » DVI to VGA
- » Thunderbolt to DVI
- » PS/2 to USB
- » USB to Serial



- » HDMI to VGA
- » USB to HDMI
- » Mini DisplayPort to DisplayPort
- » Mini HDMI to HDMI

You can examine some of these adapters in [Figure 1-9](#).



**FIGURE 1-9:** USB to Ethernet; DisplayPort to VGA, HDMI, and DVI; and two DVI to VGA adapters.

In some of these cases, the conversion is passive, while other cases, you require an active and powered device to make the conversion of signals. The CompTIA A+ objectives call out three adapters, but keep in mind that there are many more options available to you. The objectives specify the following adapters:

- » DVI to HDMI
- » DVI to VGA
- » USB to Ethernet

## ***DVI to HDMI***

On the cable, DVI and HDMI use the same digital signaling protocol, meaning that in order to implement a converter or adapter for these two connections, you only need to be able to remap the pins within the



connector. This allows for converting the plugs with very little complexity.

### ***DVI to VGA***

VGA is an analog system, while DVI is primarily a digital system, but it supports an analog signal over the same connector if you are using DVI-I or DVI-A connectors. That means if you have a DVI on one end of the connection and VGA on the end, you can display video using the analog or VGA signal. As with the DVI to HDMI adapter, this is an easy conversion to perform.

### ***USB to Ethernet***

Modern laptops and tablets have gotten smaller and smaller, and to go along with that size change is the removal of the Ethernet port. This port has a fixed height, and in order to support it, devices must be a certain thickness. To remove that thickness limitation, the only option is to remove the Ethernet port, but in doing so, the ability for the device to be directly connected to an Ethernet network is removed. The prevalence of WiFi networks eliminates that need most of the time, but for the occasions when the connection is needed, there is the multifunctional USB port. The USB to Ethernet adapter, unlike the DVI to HDMI adapter or the DVI to VGA adapter, is a small network card in a small container, powered by USB, that transfers the Ethernet data to the USB data bus.

## ***Getting an A+***

In this chapter, you examine the role of different types of connectors. In the process, you discover the differences between Thunderbolt, Lightning, and USB communication, as well as the differences between PATA, SATA, and SCSI drive interfaces. You find out about the different types of cables and connectors that are used in different areas of a computer system. You should now have a general understanding about where and why different cables and connectors are used in your system.

## ***Prep Test***

- 1. Which of the following ports offers the fastest throughput or transfer speed?**
  - (A) Serial
  - (B) Parallel
  - (C) USB
  - (D) COM
  
- 2. You are in charge of purchasing a new projector for the conference room in your office. What type of interfaces should you consider? Select all that apply.**
  - (A) USB
  - (B) HDMI
  - (C) SATA
  - (D) VGA
  
- 3. What type of port uses a three-row DB-15 connector?**
  - (A) Serial
  - (B) SVGA
  - (C) Parallel
  - (D) Game
  
- 4. DB-9 is a connector associated with which type of port?**
  - (A) Serial
  - (B) Parallel
  - (C) SCSI
  - (D) SATA
  
- 5. You have a new laptop which has a Thunderbolt port and plan to connect to a Thunderbolt dock. What is the maximum power consumption that your new laptop can possibly draw? Select the best answer.**

- (A) 20A
- (B) 60W
- (C) 100W
- (D) 150W

**6. Which interface technology is typical when attaching hard drives to a server?**

- (A) eSATA
- (B) PATA
- (C) SATA
- (D) SCSI

**7. You are looking for a new peripheral bus that supports data transfer, DisplayPort, and HDMI signals. Which peripheral bus should you consider?**

- (A) Lightning
- (B) Thunderbolt
- (C) DVI
- (D) USB

**8. Which type of video standard carries both digital and analog signals?**

- (A) HDMI
- (B) VGA
- (C) DVI
- (D) DisplayPort

**9. Monitors usually connect to a computer through what type of connector?**

- (A) DB-15
- (B) DB-25

- (C) USB
- (D) RS-232

**10. Pin 1 on a ribbon cable is usually identified by what?**

- (A) The number 1 inscribed on the connector
- (B) A colored line on the wire leading to it
- (C) A keyed connector
- (D) Pin 1 is always on the left side of the connectors

## *Answers*

1. **C.** USB offers the highest transfer rates. USB 1.1 has transfer rates of 12 Mbps, USB 2.0 offers transfer rates of 480 Mbps, and USB 3.0 offers transfer rates of 5 Gbps. See “[USB](#).”
2. **B, D.** Video interfaces which could be used for a projector include VGA, HDMI, DisplayPort, and DVI. Review “[Video Cables](#).”
3. **B.** VGA and SVGA use HD DB-15 connectors that have three rows of five pins. Take a look at “[VGA](#).”
4. **A.** DB-9 is one of the standard connectors associated with the serial port. Peek at “*Serial connectors*.”
5. **C.** The maximum power provided through the Thunderbolt is 100W. Look over “[Thunderbolt](#).”
6. **D.** SCSI is the main technology used on servers, with the latest connection types being FC (Fiber Channel) and SAS (Serial Attached SCSI). Study “[SCSI](#).”
7. **B.** Thunderbolt is a bus which is capable of supporting USB data signals as well as both DisplayPort, HDMI, and DVI signals. Refer to “[Video Cables](#).”
8. **C.** DVI is a technology which carries both digital and analog signals when using DVI-I connectors. Examine “[DVI](#).”

9. **A.** VGA and SVGA monitors usually connect to your computer via a high-density DB-15 connector. *Review “[VGA](#).”*
10. **B.** Pin 1 is identified by a colored line on the side of the cable that contains Pin 1. Keyed connectors prevent you from putting the cable in the wrong way but do not specifically identify pin 1. *Take a look at “[IDE](#).”*

# Chapter 2

## Installing and Configuring Input Devices

---

### IN THIS CHAPTER

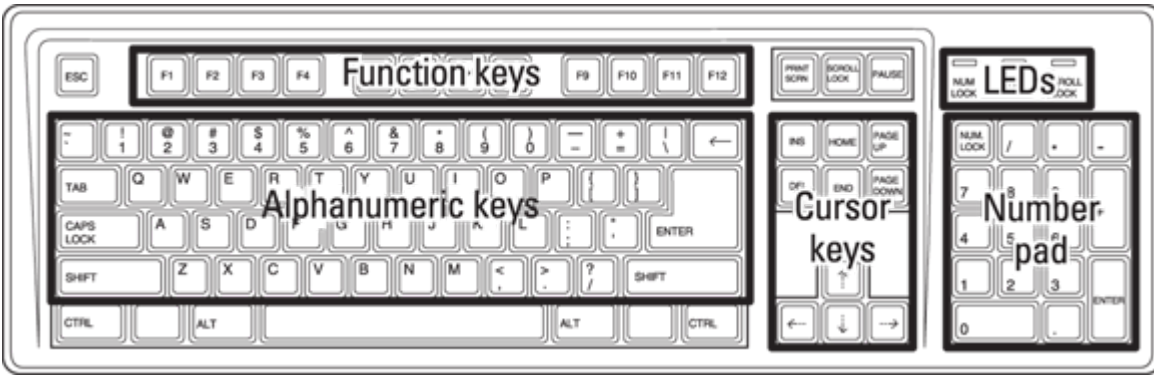
- » Understanding keyboards
  - » Working with the mouse
  - » Working with modems and network cards
  - » Looking at other input devices
  - » Understanding system resources
- 

A computer's job is to process information, but only after someone inputs that information into the system. In this chapter, I discuss different types of devices used to input data into the computer.

At anyone's disposal are many forms of input devices with which you can communicate with the computer, such as modems, network cards, touch pads, and biometric devices. A keyboard and a mouse, though, are the most popular.

### *Minding Your Keys and Qs*

The keyboard is the main device you use to interact with a computer system. Keystrokes are converted into the characters that you see onscreen, and maybe eventually print. Most keyboards have five major key parts, or groups, that contain keys grouped by specific purpose. These areas (standard desktop keyboard) are shown in [Figure 2-1](#).



**FIGURE 2-1:** The five major keyboard key groupings.

The five major groupings on a keyboard are

- » **Alphanumeric:** The *alphanumeric* keys are the keys on the keyboard that contain the letters of the alphabet, numerals, and punctuation.
- » **Function:** The 12 function keys on a keyboard offer special features. For example, in Windows, pressing F2 renames a file or icon.
- » **Cursor:** Use the cursor keys to move the cursor or insertion point.
- » **Numeric:** The numeric keypad has the mathematical operators and numbers for quick, single-handed access for inputting numeric information.
- » **LEDs:** The LEDs indicate whether features such as Caps Lock, Num Lock, and Scroll Lock are turned on or off.

Each key on the keyboard has a *keyswitch* that closes an electrical circuit on a grid when a key is pressed. When the key contacts the grid, the keyboard controller detects the keystroke and generates a *keycode*. The keycode is then converted into an ASCII code that is used to display the character onscreen.

Each location on the grid corresponds to a specific keycode. This is why you can't simply move a keycap and expect to move the character as well. For example, the letter *A* is on the left side of the keyboard. Simply moving the A keycap to the right side of the keyboard will not allow you to press that key to type the letter *A* because the location on the grid that generates a keycode for letter *A* is on the left side of the keyboard.

Different keyboards work in different ways when you press a key. Each manufacturer decides what type of keyboard to manufacture and how the keystrokes will be interpreted by the system. The two most popular techniques used to identify what keys are being pressed are

- » **Switch-based:** Uses micro-switches for each key. The keys deteriorate with time and tend to get dirty, but these keyboards are inexpensive. Call it retro, but there's still quite a market out there for mechanical switch keyboards. Expect to pay a premium for this type of keyboard, though. It's interesting how circular technology is!
- » **Capacitive:** Also known as *membrane keyboards* and are more expensive than switch-based keyboards. Despite their higher cost, though, capacitive keyboards are more reliable. Each key pushes a spring, which pushes a paddle to create an impression on the capacitive surface located under the keyboard. The impression on the capacitive surface sends a signal that is interpreted by the keyboard controller. This is the most common type of keyboard in laptops and netbooks.

For a keyboard to work with a system, software must be employed that drives the keyboard actions. Two types of software routines are used to allow the keyboard to work with the system:

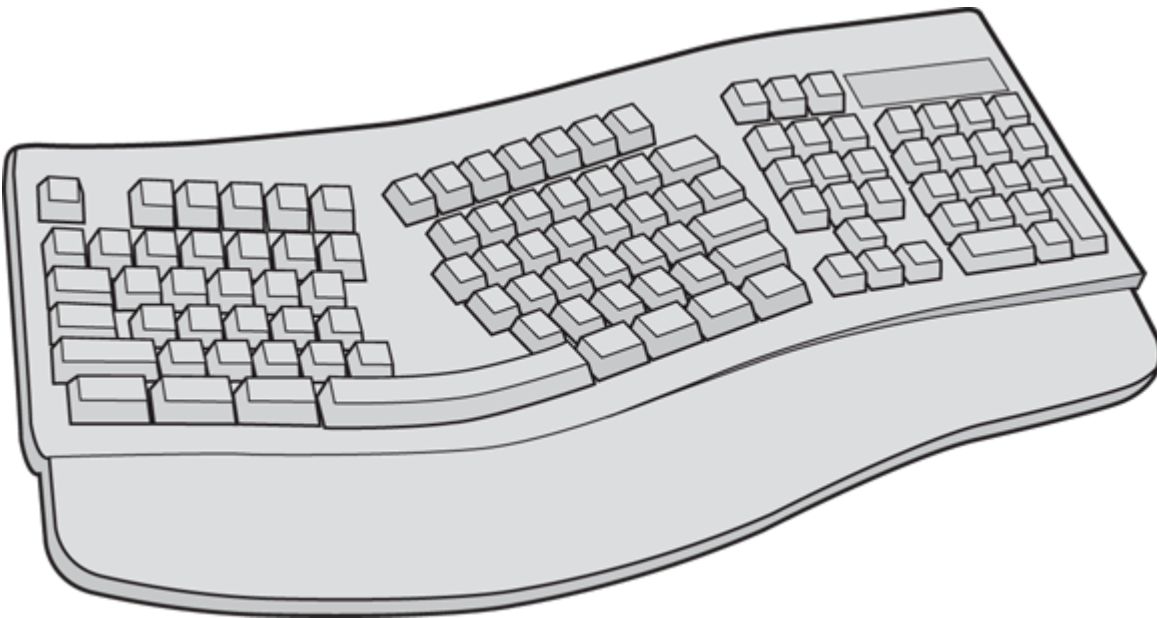
- » **Keyboard device driver:** Like any piece of hardware, a driver in Windows is responsible for allowing the device to work in Windows — including the keyboard.
- » **Firmware:** The keyboard firmware is typically stored in ROM in the actual keyboard (as in the case of an XT keyboard) or in a chip on the motherboard. The firmware contains low-level code to communicate with the hardware.

## *Identifying keyboard types*

A number of different types of keyboards have been used over time. The following list identifies the different types of keyboards you need to know for the A+ Certification Exams:



- » **Enhanced keyboard:** The enhanced keyboard is the popular keyboard used today, with 101 keys and 12 function keys. The enhanced keyboard has a numeric keypad along with cursor control keys located on the right side. The enhanced keyboard typically uses a wired USB connection.
- » **Windows keyboard:** A Windows keyboard is similar to an enhanced 101-key keyboard, but the 104-key Windows keyboard contains buttons, or keys, that control features of Windows. For example, a Windows keyboard features a button to bring up the Start menu and also a key to bring up the shortcut menu (as if you had right-clicked with the mouse).
- » **Natural, or ergonomic, keyboards:** Natural, or ergonomic, keyboards are a modification of the enhanced keyboards. A natural keyboard separates the alphanumeric keys into two parts: one part for the left hand and the other for the right hand. The keyboard is bowed and might even come apart to allow for more natural hand placement. These keyboards normally also have a wrist rest to help hands sit in a more natural position. These keyboards are designed to reduce repetitive stress injuries. [Figure 2-2](#) shows a typical natural keyboard.



**FIGURE 2-2:** A natural, ergonomic-style keyboard.

## *Installing a keyboard*

Installing a keyboard is fairly straightforward. You pretty much plug just the keyboard into the system, and Windows uses a keyboard driver to communicate with the device.



FOR THE  
EXAM

For the A+ exams, know the different keyboard connectors, as described in the following list:

- » **PS/2 connector:** A PS/2 connector — also known as a mini-DIN 6 connector — has been the most popular keyboard connector found on computers in the past but has been replaced by the USB connector.
- » **USB connector:** Keyboards that connect to the system via a USB connector have become very popular. A number of systems today are getting away from the PS/2 connections for keyboards and mice and using USB.

## *Configuring keyboards and setting accessibility options*

Configuring a keyboard in Windows doesn't involve a lot of options. Typically, you just plug it in, and it works. Windows does allow you to configure the blink rate of the cursor and also change the *repeat rate*, which dictates how quickly a letter will repeat if you hold down a key on your keyboard.

To configure the keyboard options in Windows 10, follow these steps:

1. **Choose Start, type keyboard, and select the Keyboard (Control Panel) match.**

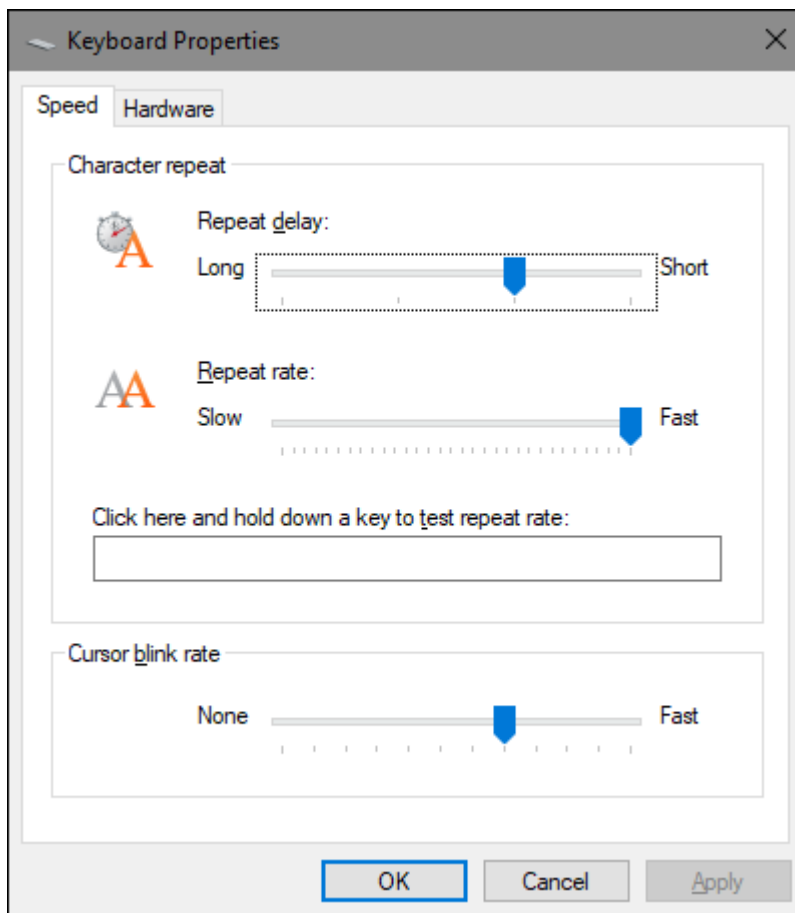
The Keyboard Properties dialog box appears, as shown in [Figure 2-3](#).

2. **Adjust the settings to suit your needs.**

Here, you can configure the character repeat options and the cursor blink rate. The following options are available:

- *Repeat Delay*: Repeat delay controls the length of time between when you first hold down a key and when the character begins to repeat onscreen.
- *Repeat Rate*: Repeat rate controls how quickly additional characters are displayed when the key is held down.
- *Cursor Blink Rate*: Cursor blink rate controls how fast the cursor blinks.

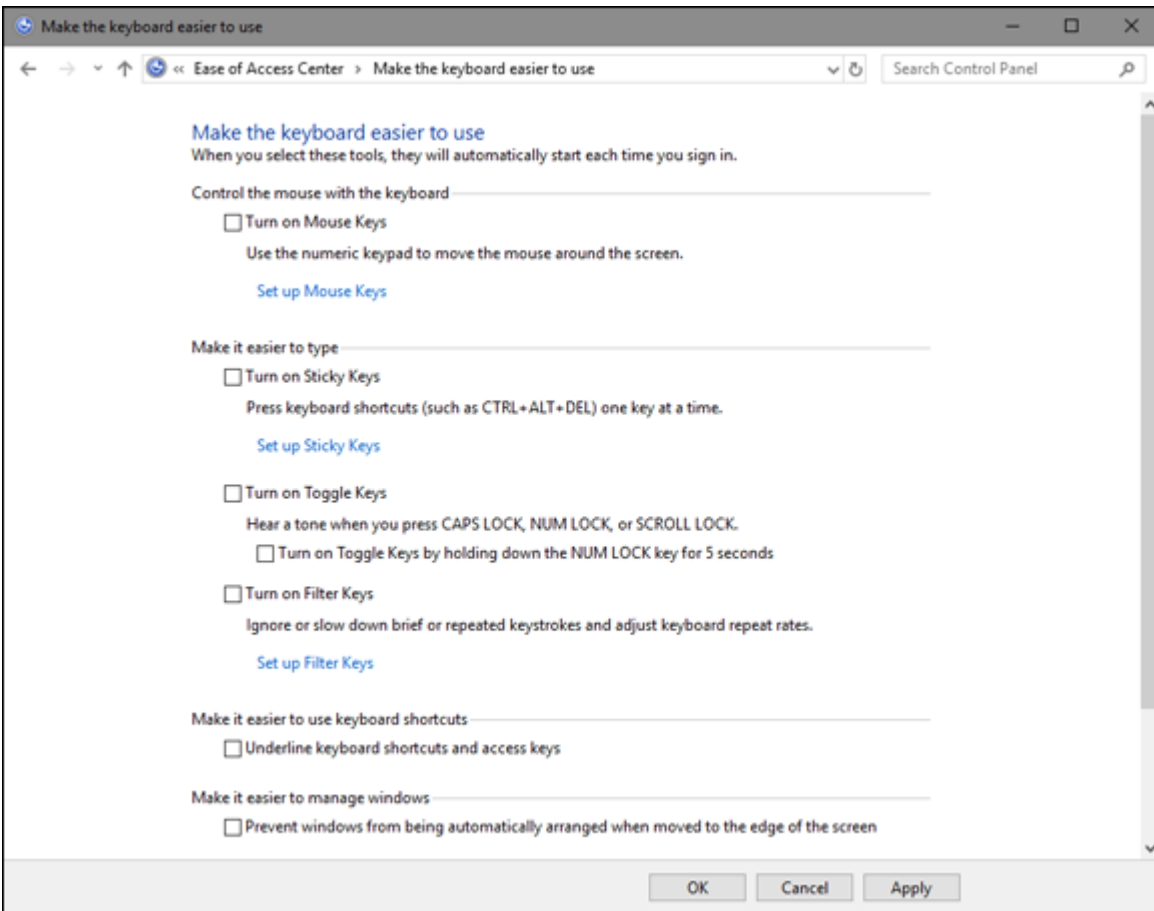
3. Click **OK** to apply your settings and close the dialog box.



**FIGURE 2-3:** Change keyboard properties through the Windows 10 Control Panel.

A number of accessibility features are available in Windows that are controlled via the keyboard. Accessibility features in Windows are designed for users who have disabilities. To configure the keyboard accessibility options in Windows 10, follow these steps:

1. **Choose Start, type keyboard, and select the Keyboard (Control Panel) match.**
2. **As shown in [Figure 2-4](#), configure the following options as needed:**
  - *StickyKeys*: This feature aids folks with an issue pressing two keys at the same time, such as Ctrl+C. Here is how it works (with StickyKeys enabled). When you press the Shift, Ctrl, or Alt key — or, if you have a Windows keyboard, the Windows key — that key remains active, as if you were holding it down, while you choose the next keystroke. If you press a key, such as the Shift key, twice then the key stays on until you press it again. Because pressing the key keeps the key held after you let go, if you wanted to perform a keystroke operation such as Ctrl+Alt+Delete with sticky keys you would simply press Ctrl, then press Alt and finally press the Delete key on its own.
  - *FilterKeys*: Use FilterKeys to tell Windows to ignore repeated keystrokes. For example, if you hold down a key too long with FilterKeys enabled, the repeat rate of the keystroke is reduced. This prevents a character from appearing many times at a quick rate.
  - *ToggleKeys*: Enabling the ToggleKeys option triggers audible tones when the Caps Lock, Num Lock, or Scroll Lock keys are pressed.
3. **Click OK.**



**FIGURE 2-4:** Change the keyboard accessibility options in Windows 10.

## *Catching the Mouse*

The other popular input device found on computer systems today is the mouse. The mouse is one of the primary input devices because of the graphical user interface (GUI) features of today's operating systems. The following sections identify the different types of mice and how to install them.

### *Types of mice*

You can find three types of mice on today's desktop computer systems: mechanical mice, opto-mechanical mice, and optical mice.

- » **Mechanical:** A mechanical mouse was the only type of mouse used with computers for many years. The mechanical mouse uses a rubber

ball that moves a pair of wheels inside the mouse. The internal wheels capture the horizontal and vertical movements of the mouse and then send that information to the computer. The movement is then displayed onscreen.

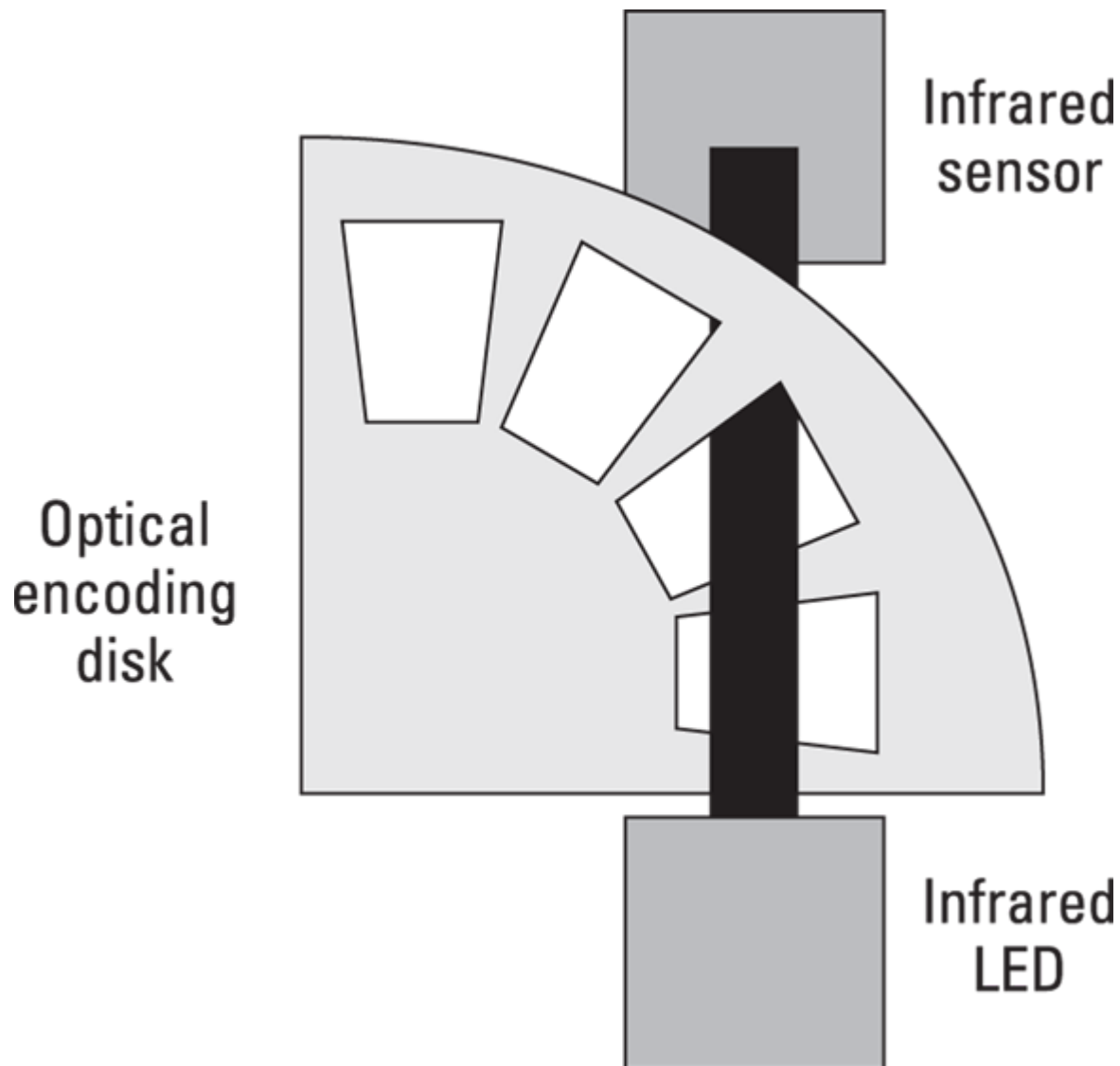
- » **Opto-mechanical:** The opto-mechanical mouse is a very popular mouse today. It uses a rubber ball that moves rollers that control the movement of a disc — the encoding disc — which has holes along the side of it.

The prefix “opto” comes into play because LEDs and sensors use an infrared light beam to determine the movement of the mouse. See [Figure 2-5](#). When the rubber ball moves the encoding disc, the infrared beam passes through the holes on the encoding disc, indicating that the mouse has moved and in which direction.

- » **Optical:** An optical mouse differs from an opto-mechanical mouse because an optical mouse has no moving parts. The rubber ball and wheels are replaced with an optical scanning system that works on pretty much any surface.

The optical scanning system is made up of optical sensors and a Digital Signal Processor (DSP). An optical mouse captures images of the surface at a rate of 1,500 images per second. The DSP then analyzes and compares the images to detect the mouse movement.

- » **Wireless:** Most mice in use nowadays connect wirelessly to their host computer. In the marketplace you’ll find a preponderance of Bluetooth-powered wireless mice, but there’s still quite a bit of infrared hardware in use today.



**FIGURE 2-5:** As the mouse moves, the holes and solid areas of the encoding disc help determine movement.

## *Installing a mouse*

Installing a mouse is very similar and just as easy as installing a keyboard. You pretty much just plug in the mouse, and the Windows mouse driver controls the device. The following is a list of the different types of interfaces you may use to connect a mouse to the system:

- » **PS/2:** One of the most popular interfaces for a mouse on desktop computers is a PS/2 connection. A PS/2 connection is also known as a mini-DIN 6 connector. Nowadays the only situations where you'll

encounter PS/2 mice or keyboards are (a) ancient point-of-sale (POS) systems in stores; and (b) older servers in data centers.

- » **USB:** The most popular type of connection for mice today is the USB connector. Simply plug the mouse into the USB port and click away! As you find out in many chapters of this book, USB is *hot-swappable* — meaning that you can plug and unplug a USB device without shutting down the system. USB can transfer data at 12 Mbps (USB 1.1), 480 Mbps (USB 2.0), or 5 Gbps (USB 3.0).



**TIP**

More and more, today's systems are using wireless keyboards and mice, which use a USB wireless adapter that connects to the computer that is responsible for receiving the signals from the wireless keyboard or mouse. The wireless signal is sent through radio frequency or via infrared depending on the keyboard or mouse. For more information on wireless, check out Book 8, [Chapter 2](#).

## *Communicating with Network Adapters*

In this section, you find out about installing network cards that allow computer systems to communicate with other systems on the network.

### *Working with network adapters*

The most popular communication device found in computers today is a network card. A *network card* is a device that allows you to connect your computer to a network or the Internet, and is responsible for sending and receiving data on the network. Not only are network cards popular in systems found in the corporate world, but because of the popularity of high-speed Internet, you can also find them in a lot of home computers as well.



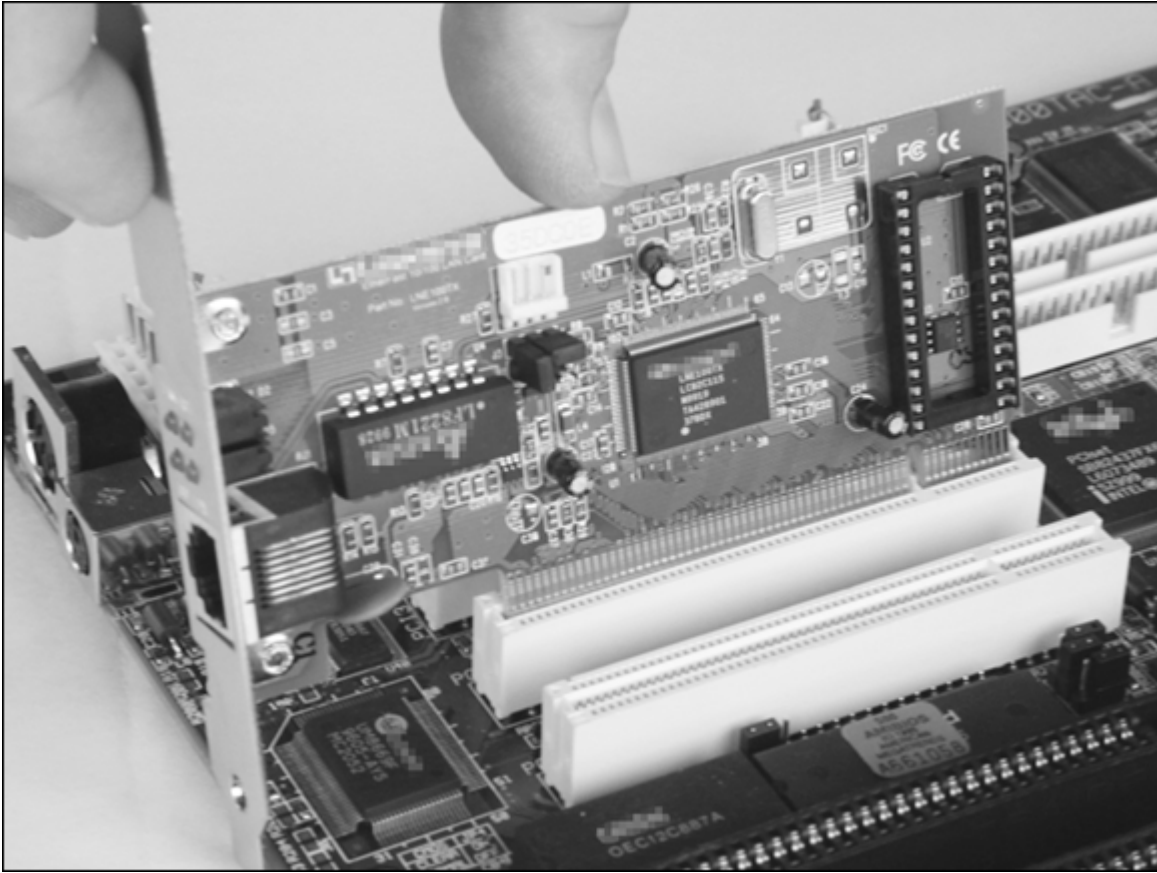
Network cards are categorized by their transfer rates. For example, a network card that can transfer 100 million bits of data per second is a 100 Mbps network card, and a network card that can transfer 1,000 million bits per second is a 1000 Mbps network card.



**TIP** The card will run at the highest common speed available between the two communicating devices. For example, if you connect your system to a 100 Mbps network switch but your system has a 1000 Mbps network card, your card will run at only 100 Mbps. This is why most systems have what is called a *100/1000 network card* — the card can talk at either 100 Mbps or 1000 Mbps.

### ***Installing a network adapter card***

When installing a network card, you first need to determine what type of interface you want to use. There are a number of types of network cards that could be installed into the system. For example, you could install a USB network card, or a PCI/PCIe network card (shown in [Figure 2-6](#)) that is inserted into a PCI or PCIe slot.



**FIGURE 2-6:** Installing a PCI network card into the PCI slot of a computer.

To install a network adapter, follow these steps:

1. **Power-off the computer and be sure to ground yourself.**
2. **Remove the cover from the computer.**
3. **If necessary, remove the blanking plate that allows access to the modem from the back of the PC.**

This allows the network card to fit in the slot.

4. **Place the network card into the appropriate expansion slot.**

For example, you will most likely have a PCI Express (PCIe) card, so place the PCIe network card into an available PCIe slot.

5. **Screw the network card into place and put the cover back on the PC.**
6. **Connect the network cable to the back of the network card.**

## 7. Power-on the PC.

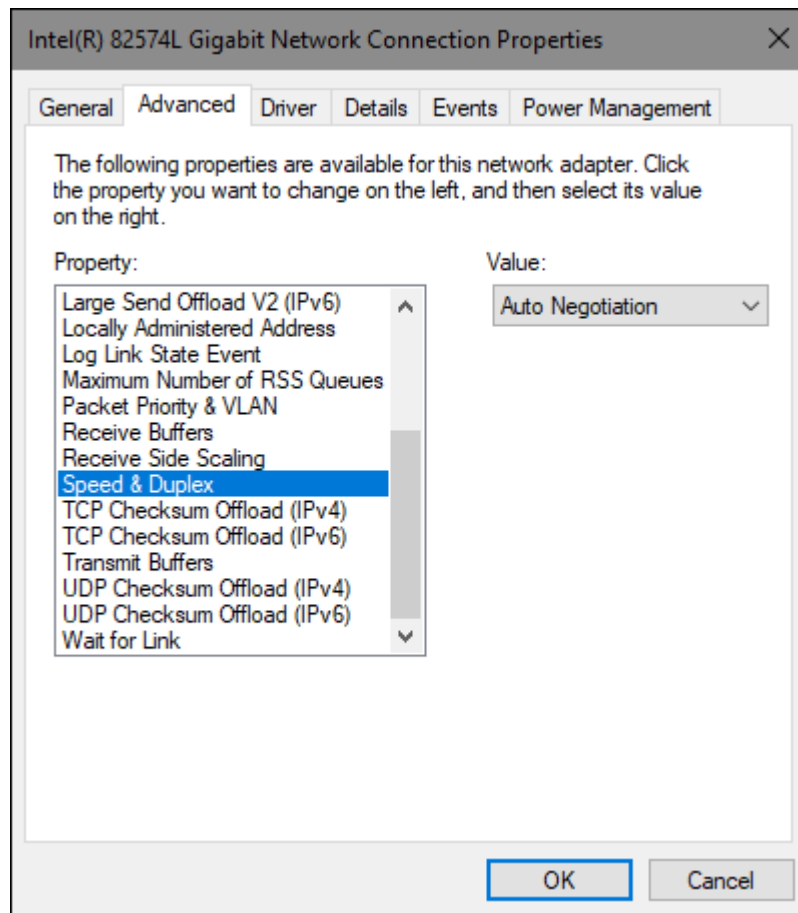
### *Configuring a network card*

After you install the network card, Plug and Play should kick in and either load the driver for you or prompt you for the driver. When the driver is loaded, you can specify settings for the network card in Windows. For example, if you want to force your network card to run at a particular speed, you can do that through the properties of the network card.

To configure your network card in Windows 10, follow these steps:

1. **Click Start, type device manager, and select the Device Manager (Control Panel) result.**
2. **In Device Manager, expand the Network Adapters category on the left, right-click your network card, and then choose Properties.**
3. **In the Properties dialog box for the network card, click the Advanced tab to see settings that can be configured for the network card (shown in [Figure 2-7](#)).**

The advanced settings are different for each make and model of network card because the settings are particular to the driver that is loaded. A very popular setting is the link speed, which specifies what speed you want to run the card at. Most network cards are set to Auto, which means the card will detect the best speed. When troubleshooting, though, you can force a particular speed.



**FIGURE 2-7:** Configuring network card settings through Windows Device Manager in Windows 10.

## *Special-purpose network adapters*

Let's take a look at some other means of attaining network connectivity. Nowadays it's not at all safe to assume that we'll connect to the Internet only from a full desktop or even laptop computer.

Instead, most people access the World Wide Web, their email, and instant message accounts from their smartphones or tablet devices. That said, the following examples all apply to traditional computers.

In general, these special-purpose network adapters use the USB standard for maximum flexibility, although you can always purchase a PCIe variant if you need to install the card inside your computer case.

» **Wireless cards:** A wireless card uses the IEEE 802.11 protocols to connect your compute to a local area network and potentially the

Internet. The form factor for WiFi cards has become almost inconceivably small.

- » **Cellular cards:** A cellular card is associated with a particular cellular service provider such as AT&T or Verizon. Thus, you need to have a cellular data plan account in order to make use of these expansion cards.
- » **Modem cards:** Believe it or not, some people still connect to the Internet via dial-up modems. To accommodate this, analog modem cards remain available, although you'll probably need to order them online.
- » **FireWire cards:** Recall that FireWire can be used for TCP/IP networking in addition to multimedia data transfer. The IEEE 1394 standard describes the FireWire standard.
- » **Thunderbolt cards:** Similar to FireWire, the Apple Thunderbolt media technology not only can carry video, but also data. For example, you can quickly send data from one Mac to another by using an Apple Thunderbolt data cable.

## *Other Input Devices*

As technology moves on, new input devices appear. For example, laptops use a touch pad as an input device, whereas handheld devices use a pen-like stylus. The following is a list of input devices you might encounter:

- » **Touch pad:** A number of laptop systems today use a touch pad as an alternative way to control the mouse pointer in Windows. The *touch pad* — that rectangular area found below the keyboard that you move your finger(s) across to move the mouse pointer — also usually bears two buttons below the square to perform left- and right-click operations. A touch pad is displayed in [Figure 2-8](#).
- » **Touch screens:** You see touch screens used a lot at public terminals for things like information booths and bank machines. *Touch screens* require that you actually touch the screen to choose different options.

- » **Barcode reader:** A *barcode reader* is a type of scanner that reads bar codes and then converts the bar code into data stored on a computer and used in applications. An inventory application is an example of an application that uses a barcode reader as an input device.
- » **Biometric devices:** *Biometric devices* are used to authenticate, or log, people onto a system by using biological characteristics of that person, such as a fingerprint or a retinal scan. Biometric devices are very popular in high-security environments because of how difficult it is to impersonate someone when dealing with authentication methods such as a fingerprint scan. Some laptop makers are even starting to include fingerprint scanners in consumer-level laptops as security devices and theft deterrents.
- » **Scanner:** A scanner is used to capture the contents of a document or real-life object and generate an image of the object on the computer that is connected to the scanner. You find out more about scanners in Book 3, [Chapter 5](#).
- » **Bluetooth:** Bluetooth is a popular short-range (30 feet or so) wireless protocol that's used all the time nowadays. For example, I'll bet that your hands-free headset or your wireless speakers use Bluetooth connectivity.
- » **Smart TV:** A smart TV is a high-definition television that is Internet-connected thanks to an integrated wired or wireless network adapter. Normally smart TVs are set up to access paid media services such as Netflix or Hulu. You can also typically stream multimedia content from your computer or smartphone directly to the smart TV.
- » **Set-top box:** If you have digital cable service, then you may use a set-top box to access the cable network. Other examples of set-top boxes are the Apple TV and Roku; these devices allow you to stream multimedia from the Internet through the set-top box and ultimately to your HDTV.
- » **USB cards:** A PCIe USB interface presents a permanent alternative to a plug-in USB hub.

- » **Storage cards:** This is a vague exam objective (thanks, CompTIA!). By “storage card” I envision a PCIe SATA card that allows you to expand the internal storage of a computer. Alternatively, we could be talking about a PCIe card that connects a server to an external disk array or storage area network (SAN).
- » **KVM:** A KVM switch is a device that allows you to connect a single keyboard, mouse, and monitor to the KVM switch. The KVM switch is then connected to multiple computers so that you can use the one set of keyboard, mouse, and monitor to switch among multiple computers. I use this in my office because I have three computers but do not want to have to physically use three different keyboards, mice, and monitors. I simply press the toggle button on the KVM switch and it changes which computer I am viewing on the screen and managing with the keyboard and mouse.
- » **Microphone:** The microphone is used to create audio input on the system. The microphone is connected to the microphone port on the system and can be used with recording software to record your voice.
- » **Game pads and joysticks:** A game pad is also known as a control pad and is a device similar to a controller for a video game console like an Xbox One or PlayStation 4. Just as those controllers allow you to navigate through the games on a console, a game pad can provide input to a computer as well. Another common input device with games on the computer is the joystick: a device that has a stick used to navigate and typically has a button on the base.

Modern day game consoles almost always ship with wireless game pad controllers; Bluetooth is the most popular connection method.
- » **Digitizer:** A digitizer is a device that is used to create a digital form of information that is not on the computer. For example, if you have some old books or documents, you can create electronic documents out of them with a digitizer. You can also find digitizers to convert old reel-to-reel movies, VHS movies, and cassette tapes to electronic files.



**FIGURE 2-8:** A touch pad is a popular input device to control the mouse pointer on a laptop computer.

This chapter discusses installing a network card into the system, but a number of other types of cards can be installed. The process to install any kind of expansion card into the system is the same as installing a network card. The following are other types of expansion cards you may need to install:

- » **Flash storage cards:** Many computers today have a way to connect storage cards or memory cards to the system. If your system did not come with card readers, you can purchase and install a storage card reader to allow you to insert different types of memory cards.
- » **Riser cards:** A riser card is connected directly to the motherboard and “rises up” from the motherboard. It is its own board that has a number of expansion slots on it so that you can add other types of cards to the system.



- » **Smart card reader:** A smart card is a plastic wafer about the same size as a credit card that includes integrated circuit (IC) technology. Most commonly, smart cards and their associated readers are used to authenticate users, open doors, and the like.
- » **Motion sensor:** Motion sensors typically use infrared technology to detect movement. You see motion sensors in residential and commercial security systems.
- » **MIDI-enabled device:** By installing a Musical Instrument Device Interface (MIDI) expansion card in your PC, you can connect MIDI-enabled devices such as guitars or keyboards. You'll then be able to send musical signals from the MIDI-enabled device through the MIDI interface card into the computer.

## *Getting an A+*

In this chapter, you find out about different types of input devices. The following list outlines some of the key points to remember for the A+ exams:

- » Keyboards usually connect to the system with a USB connection with today's systems.
- » Most mice today connect to the system via a USB port wirelessly with Bluetooth or Infrared.
- » Network cards are the most popular type of communication device in today's systems. Be sure to review the networking chapters to fully understand how to network a system.
- » Many new input devices have sprung up over the last few years, so make sure you enter your 1000-series A+ exam session fully up-to-speed. You need to be able to recognize and apply devices like cellular cards and storage cards to modern-day computer troubleshooting situations.

## *Prep Test*

**1. At what speed does USB 2.0 transfer information?**

- (A) 5 Gbps
- (B) 12 Gbps
- (C) 100 Mbps
- (D) 480 Mbps

**2. Which type of keyboard is designed to reduce repetitive stress injuries?**

- (A) AT keyboard
- (B) Natural keyboard
- (C) Windows keyboard
- (D) Enhanced keyboard

**3. The StickyKeys feature instructs Windows to ignore repeated keystrokes.**

- (A) True
- (B) False

**4. At what speed does USB 3.0 transfer information?**

- (A) 12 Mbps
- (B) 480 Mbps
- (C) 5 Gbps
- (D) 480 Gbps

**5. Which two popular connector types are used with a mouse?**

- (A) USB
- (B) Parallel
- (C) Bluetooth
- (D) OS/2

**6. Which two types of interfaces are typically used to connect a network card to the system?**

- (A) Parallel
- (B) USB
- (C) PCIe
- (D) Serial

## *Answers*

1. **D.** USB 2.0 devices run at 480 Mbps. Review “[Installing a mouse.](#)”
2. **B.** Natural keyboards are a form of ergonomic keyboard that reduces repetitive stress injuries. Check out “[Identifying keyboard types.](#)”
3. **B.** The statement is false. The FilterKeys feature tells Windows to ignore repeated keystrokes. The StickyKeys feature aids folks with an issue pressing two keys at the same time. Review “[Configuring keyboards and setting accessibility options.](#)”
4. **C.** USB 3.0 runs at 5 Gbps. Peek at “[Installing a mouse.](#)”
5. **A, C.** Popular connections used by the mouse today are the USB connector and the PS/2 connector. Look over “[Installing a mouse.](#)”
6. **B, C.** Network cards connect to the system as either a USB or PCIe device. Study “[Installing a network adapter card.](#)”

# Chapter 3

## Installing and Configuring Output Devices

---

### IN THIS CHAPTER

- » Understanding video adapters and monitors
  - » Working with sound cards
  - » Looking at other output devices
- 

An *output device* sends data from the computer and creates a tangible output. Examples of output for a system are displaying information on the monitor, printing a report, or even listening to the sound that the sound card puts through the speakers when playing your favorite computer games.

This chapter also looks at the video hardware that is responsible for creating the images on the screen and discusses how a sound card works. These topics are essential to passing your A+ certification exams, so be sure to study them well!

## *Understanding Video Adapters*

A *video adapter* (also known as a video card) — the interface between the monitor and the computer — is responsible for display functions. For example, when using a CRT monitor, the video adapter is responsible for converting the digital data from the computer into analog information. The data is converted to an analog signal before being delivered to a monitor because CRT monitors use analog data to create the image.

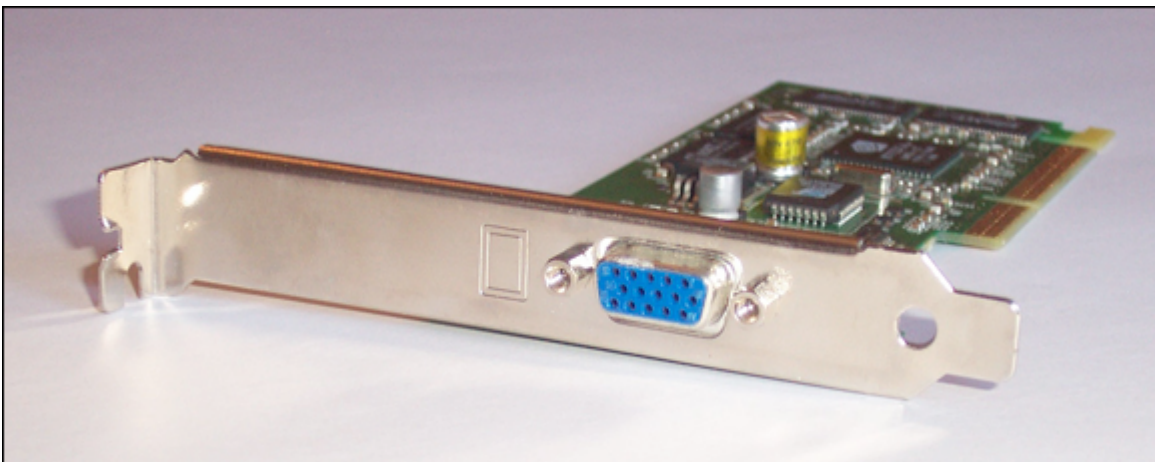
Because display functions are very time- and memory-consuming, most video adapters these days have their own processing chip and memory to

alleviate the processing workload from the CPU. Today's video adapters are typically PCIe cards, but you might run into some older systems that require a PCI or even an AGP video card because these systems don't have a PCIe slot. For more information on PCIe and AGP, check out Book 2, [Chapter 1](#).

The following outlines the basic role of what the video adapter does when it comes to displaying data on the computer screen:

1. Data is sent to the video card via the expansion bus that the video card resides in.
2. The video chipset on the video card writes the data to memory located on the card.
3. After being stored in memory, the data is passed to the *digital-to-analog converter (DAC)*, where it is converted from digital signals to analog signals that the monitor can understand.
4. The data is passed to the monitor, which then displays the data on the screen.

The video adapter is identifiable by its unique 15-pin female connector, comprising five pins in three rows. On most systems today, HDMI or DVI ports are much more common than VGA, although VGA continues to exist like a dinosaur that evaded extinction. [Figure 3-1](#) shows a video port.



**FIGURE 3-1:** Looking at the back of a video card and the port style.

## *Looking at the video standards*

A number of video standards have been developed over the years, with each standard increasing the quality of the display from the previous standards. The quality of display is measured by the resolution and color support.



FOR THE  
EXAM

The following list outlines some of the popular video standards, which you need to know for the A+ certification exams:

- » **Monochrome Display Adapter (MDA):** Displays data in a text format with a single color — white text on the black screen. This standard is pretty much obsolete, but you might encounter an old server that still uses it.
- » **Color Graphics Adapter (CGA):** The next step above MDA; supports four colors in a 320 x 200 resolution but supports only two colors with a resolution of 640 x 200. CGA video adapters were the first adapters to support color.
- » **Enhanced Graphics Adapter (EGA):** The next step after CGA; much improved over the CGA graphics standard. EGA supports 16 colors at 640 x 350 resolution.
- » **Video Graphics Array (VGA):** Video graphics standard that allows for a resolution of 640 x 480 with 16 colors, but also supports 256 colors at lower resolutions.
- » **Extended Graphics Array (XGA):** Graphics standard that supports resolution of 800 x 600 with 65,536 colors, or a resolution of 1024 x 768 with 256 colors. There are many different spin-offs of the XGA video standard, including Wide XGA (1366 x 768), XGA+ (1152 x 864), and Wide XGA+ (1440 x 900).
- » **Super VGA (SVGA):** Supports 16 million colors at resolutions as high as 1280 x 1024; a popular graphics standard for many years.

- » **Super XGA+:** A popular video standard for LCD displays on laptop computers supporting a resolution of 1400 x 1050. The widescreen version (WSXGA+) supports a resolution of 1680 x 1050.
- » **Ultra XGA:** Supports resolution of 1600 x 1200; the video standard for 20-inch or 21-inch LCD displays on laptop computers.
- » **WUXGA:** *Widescreen Ultra Extended Graphics Array* (WUXGA) supports a resolution of 1920 x 1200 and is the widescreen version of the UXGA standard. This video standard is popular with widescreen LCD televisions and computer monitors.

## *Aspect ratios*

A monitor's *aspect ratio* is simply the proportional relationship between the width and height of the display. Let's quickly review the most common aspect ratios found in current-generation computer displays.

- » **4:3:** This is the old aspect ratio used in CRT displays. When you display content recorded in a 4:3 ratio on a 16:9 monitor, you'll normally see black vertical bars to the left and right of the screen image.
- » **16:9:** Here the display width is practically twice its height. Movies and high-definition video normally use 16:9 resolution. When you display content recorded in 16:9 on a 4:3 display, you'll usually see black horizontal bars above and below the image; this annoying feature is known colloquially as "letterboxing."
- » **16:10:** This aspect ratio, while very similar to 16:9 widescreen, is preferred by some videographers and graphic designers because 16:10 is close to the "golden ratio." The golden ratio, which denotes an aspect ratio of 1.618, has been used throughout human history for important works of architecture, painting, book design, and so on. For reference, the decimal representation of 16:10 is 1.610.

## *Video card features*

Although a number of video standards are available as well as a wealth of video cards, some features are common to every video card. This

section outlines some important characteristics of video cards, such as resolution, colors, and video memory.

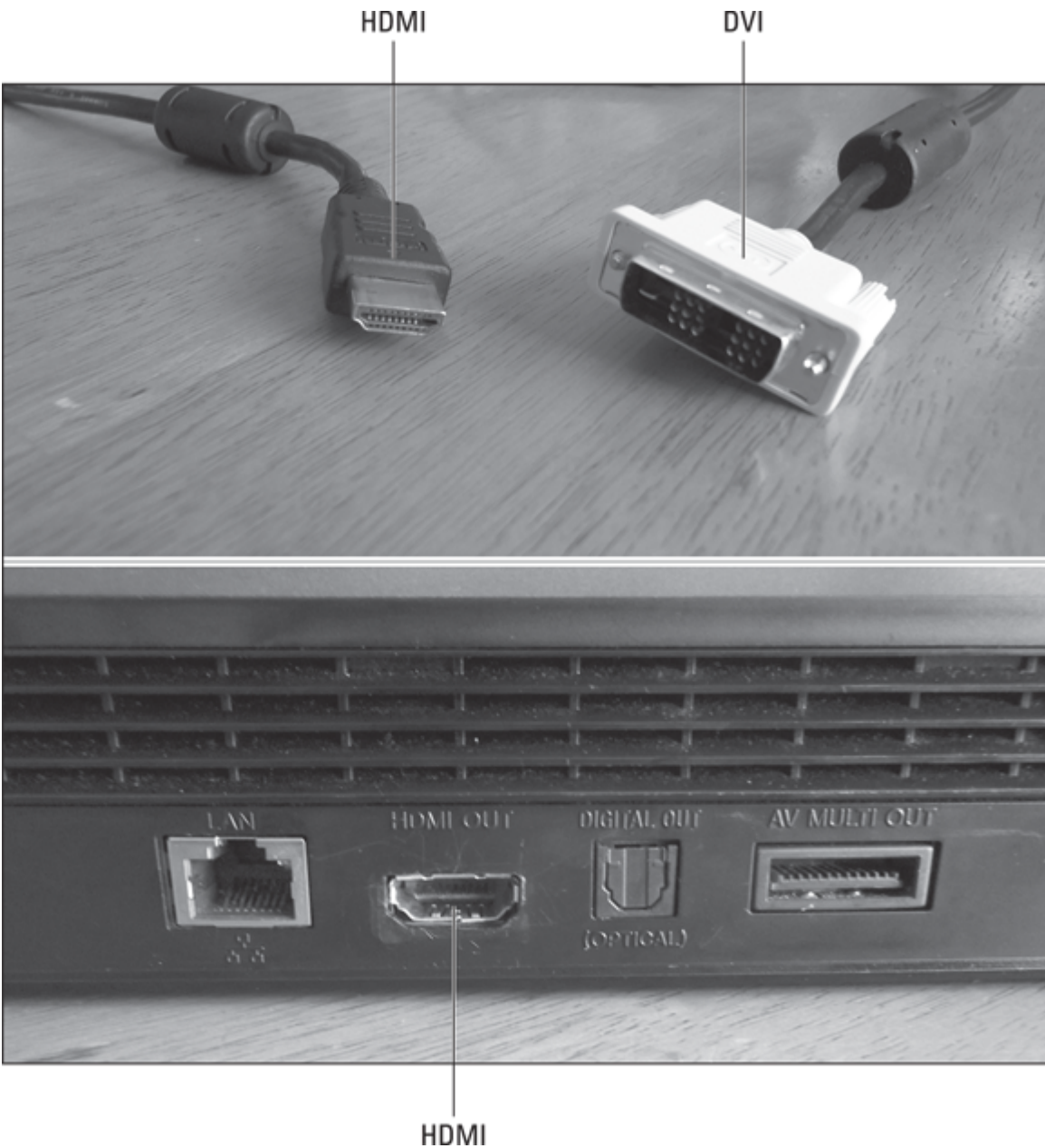
### ***Special connectors***

Most older video cards come with the typical 15-pin video port (three rows of five pins) that is usually blue in color. Today's video cards, though, typically have a number of additional connectors that can be used to connect your system to a video display. You should find that HDMI is the most common video connector interface nowadays.

The following is a listing of high-quality video connectors used by computers, video game consoles, or even projectors:

- » **S-Video:** The *Separate-Video* (S-Video) connector is designed to carry an analog video signal, using a 4-pin mini-DIN connector or a 7-pin mini-DIN connector. The S-Video standard is just designed to carry the video signal and not the audio signal.
- » **DVI:** The *digital video interface* (DVI) is a video interface standard (see [Figure 3-2](#)) designed to carry the video signal, in high-quality, uncompressed format, from a source (such as computer) to a digital display (such as an LCD monitor or a digital projector).
- » **HDMI:** The *High-Definition Multimedia Interface* (HDMI) is an audio *and* video interface designed to carry a digital signal from a source (such as a Blu-ray disc player, video game console, or computer) to a display output (such as an LCD monitor, a digital TV, or a digital audio device).





**FIGURE 3-2:** An HDMI connector (top left), a DVI connector (top right), and an HDMI port (bottom).

### ***Built-in coprocessors***

A number of new video cards have a built-in coprocessor that processes most display functions on behalf of the CPU. This allows the CPU to service other requests on the system and not have to worry about processing any video commands. These advanced video cards are also known as *accelerated video cards* or *graphics accelerator cards*.

## ***Resolution***

*Resolution* is a term that techies use to describe how functional a video card is. For example, I might brag about my video card being able to run at 1024 x 768, and you could turn around and say, “Is that all? My video card supports 1280 x 768.”

*Resolution* describes how many pixels are supported by both the video adapter and the monitor. A *pixel* is a small dot conjoined with other small dots to help create the image onscreen. The more pixels that are supported on your screen, the closer the dots must be — which gives you a finer display.

As an example, a video card that supports 1280 pixels going across the screen and 768 pixels going down the screen (1280 x 768) will create a much finer image than a video card that supports only 800 pixels going across the screen and 600 pixels going down the screen (800 x 600).

## ***Supported colors***

The picture on your monitor will look much better if the video card supports a lot of colors, so one of the other often-touted video card characteristics is how many colors the video card supports. Bottom line, the more colors the better.

If you’re curious to see what the big deal is about the number of colors supported, the steps depend on your operating system. Here’s a quick way to get a look at the difference in Windows 10. Follow these steps to change your resolution and color support:

- 1. Right-click your desktop and choose Display settings from the contextual menu.**

This takes you to the Display settings panel where you can change your screen resolution. The higher the resolution, the finer the display.

- 2. Choose your preferred resolution from the Resolution drop-down list.**
- 3. To change your color support, click the Advanced Display Settings link.**

Increasing the color support will allow the system to display more colors to you on the screen, which will enhance the image.

4. **Click the Monitor tab.**

5. **Choose your preferred color support at the bottom of the dialog box and then click OK.**

### *Video memory*

Because a video card has to process such a large amount of data, the video card comes with its own memory — *video memory*. Video memory is available in many different sizes, and popular amounts run from 1GB up to 8GB and beyond. Some video cards simply use DRAM, but because the demands of video display are so high and DRAM was so slow in the past, other memory types were developed for video:

- » **Video RAM (VRAM):** Has the benefit of being *dual ported* — it can be read from and written to simultaneously — which adds to the performance of the memory.
- » **Multibank DRAM (MDRAM):** A type of video RAM that uses the full width of the *video bus* (the expansion bus where the video card resides) with fewer memory chips.
- » **Window RAM (WRAM):** Stores its data in chunks, which makes the data transfer faster than the more-expensive VRAM. Like VRAM, WRAM is dual ported.
- » **Synchronous Graphics RAM (SGRAM):** SGRAM is a type of video memory that is *single ported*, which means that you can only read from or only write to the memory at one time. SGRAM is four times faster than other types of DRAM memory and is synchronized with the CPU clock.

Being able to change some of the video card's characteristics, such as color support or resolution, is a characteristic of the video driver that is installed. You might find that you cannot set your video card to 24-bit color because the driver does not support it. Of course, the driver does not support it because the card does not support it. Before I show you how

to change your resolution, you need to know how to install a video card, which is covered in the next section.

## *Installing a video card*

Installing a video card is like installing any other card, such as a network card or modem. You simply need to place the card into a supported bus architecture — typically PCIe — and then load the driver.

The following steps outline how to install a video card:

1. **Power-off and unplug the computer.**
2. **Open the case or side panel of the computer to access the expansion slots.**
3. **If you are replacing a video card, take out the old one.**



**TIP**

If the old video card is integrated into the motherboard, you will not be able to remove it, but you might be able to disable it in CMOS. (For more information on CMOS, check out Book 2, [Chapter 4](#).)

4. **If you are adding the first video card to the system, remove the blanking plate for the AGP or PCIe slot you want to use.**
5. **Insert the card into the slot until it fits firmly.**
6. **Screw the video card's plate into place to secure the card.**
7. **Place the cover back on the computer, plug it back in, and power it on.**

When you power-up the system, Plug and Play should kick in and detect the newly added device and either load a driver or prompt you for the driver. After the driver is loaded, you can configure the display settings discussed in the following sections.

## *Using Your Monitor or Display*

After you install the video adapter (see the previous section), you then need to connect the monitor to the video adapter. The following sections identify the different types of displays used with computers today and then discuss how to configure your display through Windows.

## *Types of displays*

You might find a few different types of displays connected to a system: a CRT monitor, an LCD monitor, or even a projector. In this chapter, I focus on CRTs because LCDs are discussed in Book 3, [Chapter 6](#), and you are not likely to get any questions on the A+ exams about projectors. I do define each type of display, though.

### *Cathode ray tube (CRT)*

CRT monitors were popular for computing for many years (and were also popular as television screens) and are typically curved screens but there are flat-screen versions. After receiving a signal from the video card, a CRT monitor displays the image by using an electron gun that shoots electrons at the phosphors covering the back of the screen, causing those areas of the screen to glow.

The electron gun located in the CRT continues to fire at the back of the screen from left to right and from top to bottom. This causes a glow of three phosphors colored red, green, and blue to create a single pixel on the screen. The combination of all the lit pixels creates the image that you see, and the speed at which the pixels change gives the illusion of moving objects onscreen.

*Refresh rate* and *dot pitch* are two very important terms used to describe a monitor. A monitor's *refresh rate* refers to how often the electron gun can redraw the entire screen. The faster it can redraw the screen, the smoother any moving objects appear.

A monitor's *dot pitch* is simply the distance (in millimeters; mm) between two pixels of the same color on a monitor. For example, an average monitor has a dot pitch of 0.28 millimeters, and a better monitor has a dot pitch as tight as 0.24mm.

### *LCD*

Liquid crystal display (LCD) — a popular flat-display type found on laptops for many years — is now a popular choice for display with desktop computers and TVs.

An LCD has two sheets of material surrounding a liquid that contains crystals that act as pixels for the display. Each crystal has a red, green, and blue cell illuminated by an electrical charge hitting the crystal, which then creates the onscreen image. You can find out more information about LCDs, such as active and passive matrix, in Book 3, [Chapter 6](#).

### ***LED and OLED Displays***

A *light-emitting diode* (LED) is like a tiny lightbulb, but has a diode in the middle of the “bulb” that emits light when charged. The benefit of LEDs is that the diode is used instead of hazardous materials such as mercury and also does not get as hot as a regular lightbulb.

An LED display is like an LCD display in the sense it is a flat-panel display type as well, but with LED displays, you can have even thinner displays than LCD, because of the small size of the LEDs in the display. LED TVs are actually LCD TVs with the use of LEDs as a backlight. The benefit of using LEDs as a backlight is that areas on the display that require darkness simply have those LEDs turned off so that the image is dark in that area. This gives you better picture quality and contrast than with a regular LCD display.

*Organic light-emitting diode* (OLED) is a type of LED that uses organic material as the semiconductor to emit the light when a charge is applied. An OLED display does not use a backlight approach, which means that it can have more control over dark areas than LED displays and better contrast.

### ***Fluorescent versus LED backlighting***

The LED display gets its name by virtue of the LED grid that serves as the monitor’s backlighting system. Older, fluorescent backlit displays normally offer poor black levels because the tiny fluorescent tubes are all on, all the time. You can often see a light “halo” around the edges of an LED-backlit display, even with an otherwise black screen.

LED LCD monitors use one of two common panel types: Twisted Nematic (TN) or In-Plane Switching (IPS). The advantage of TN LED displays is that they show response times, which is appreciated by gamers and sports TV aficionados. The selling point of IPS LED displays is their superior viewing angle.

### *Plasma*

Plasma displays are flat displays like LCDs but use a different approach to creating the image onscreen. Plasma displays create the image by having small cells of gas sitting between two plates of glass. An electrical charge is applied to the cells of gas, which then causes the cells to light.

### *Projector*

I can't really talk about display types without talking about using a projector to display the image. Screen projectors are becoming popular both for home theater systems and in company boardrooms.

When using a computer or laptop with a projector, the projector connects to the video adapter via an HDMI or VGA interface. If you are using a laptop, you might notice that the output does not emanate from the projector right away. Most laptops allow you to choose whether to display the image on the LCD, projector, or both by holding down the function (Fn) key and then pressing either F4, F5, or maybe F8 (as is the case on my laptop). Look for the function key that has a monitor on it to get your projection going.

### *Evaluating display features*

When looking for a display for your computer, laptop, or home entertainment center, there are a number of characteristics of the display that help you identify the quality of what you are purchasing. The following are key characteristics to look for when selecting a display:

- » **Refresh rate:** Specifies how frequently a display redraws the screen. Increasing the refresh rate can reduce the flicker on the screen that strains people's eyes.
- » **Resolution:** Defines how many pixels are supported on the screen — the higher the resolution, the finer the image.

- » **Native resolution:** The actual resolution of a monitor, as opposed to the display resolution, which may be set lower and scales the image to the display area of the monitor.
- » **Brightness/lumens:** Lumens is the way to measure the amount of light that is coming out of a display. It's a very common characteristic to measure projectors. For example, a projector with 2,700 lumens is brighter than a projector supporting 2,100 lumens.
- » **Color depth:** A measurement of the number of bits used to define the color of a single pixel. The higher the bit depth, the larger your monitor's color palette. Nowadays 32-bit color depth is standard, which yields a palette of 16.7 million color shades.
- » **Contrast ratio:** A value measuring the brightness of different colors, such as white versus black. The larger the ratio, the better the picture quality on the display. For example, a display with a 3000:1 ratio is a better quality than a 2000:1 ratio. In this example, the values of 3,000, 2,000, and 1 are the supported lumens of the brightest color supported versus the darkest color supported.
- » **Analog versus digital:** Many displays today will support analog and/or digital connections. When a computer is connected to an analog device such as a CRT monitor, the digital data is converted to analog data, and you may experience loss in quality compared to connecting the computer to a digital display — for example, through a DVI or HDMI connector with an LCD or LED display.
- » **Privacy/antiglare filters:** When employees sit in front of a monitor all day, they may experience eyestrain from the glare of the monitor. You can place antiglare filters on the display to help reduce the glare, along with the eyestrain and fatigue that the employee experiences.
- » **Multiple displays:** Systems today can have video cards with multiple display ports that allow you to use multiple monitors with your system. This gives you more screen space to work with. For example, you can open your email on one monitor and then work on a document in the other monitor. You can also install multiple video cards in the system to get multiple display support.





FOR THE  
EXAM

Be sure to know the characteristics of displays listed here such as refresh rate, lumens, contrast ratio, and native resolution. Also be sure to review the troubleshooting displays in the next topic.

## *Configuring your display settings*

You can change the characteristics of your display — such as color support or resolution — after the driver is loaded for your video adapter. Whatever settings you choose must be supported by both the video card and the monitor. For example, choosing too high a resolution can distort the display. In this example, the resolution is supported by the video card but not the monitor. Mismatched resolution was such a problem in the past that Windows OSes now ask you whether the display is okay when you change the resolution. If you choose Yes, the settings are applied. If you choose No or don't choose anything for a few seconds, the settings are reverted to their previous state.

To configure your display settings in Windows 10, follow these steps:

1. **Right-click your desktop and choose Display settings.**
2. **In the Resolution drop-down list, choose the resolution you want to use.**
3. **To change your color support and refresh rate, click the Advanced display settings link.**
4. **Click the Monitor tab.**
5. **Choose your color from the Color drop-down list and the refresh rate from the Screen Refresh Rate drop-down list.**
6. **Click OK.**
7. **When asked whether the display looks okay, click Yes.**

## *Configuring multidisplay support*

Windows OSes support a feature called multidisplay support, which allows you to insert multiple video cards into the system and have a monitor connected to each video card. Then, you can extend your Windows desktop to include the second monitor, allowing you to use the screen space from both monitors at the same time.

Today's video cards have multiple video ports, such as VGA, HDMI, and DVI. With many of these cards, you can use multiple ports instead of purchasing additional video cards.

With multidisplay support, you can move one program to one of the monitors and then use another program on the second monitor. For example, I place my email program on my right-hand monitor and surf the Internet on my left-hand monitor. When an email comes in, I already have the email program open, so I can simply read the email.

To configure multidisplay support in Windows, follow these steps:

1. **With your computer off, open your computer case and install an additional video adapter.**

You can find instructions for installing a video card in the earlier [“Installing a video card”](#) section.

2. **Put the computer case back on and power-on the system.**
3. **Plug a separate monitor into each of the two video cards.**
4. **Ensure that a driver is loaded for each video card and for each monitor.**
5. **Enable multi-monitors in the Display settings panel.**

Once you have enabled multidisplay support, you can then adjust the resolution and color support for each different display.

## ***Troubleshooting Display Issues***

When working with computers, you will end up troubleshooting display issues with the monitors or projectors connected to those computers. The

following are some tips that you can use when you are troubleshooting display issues:

- » **VGA mode:** If you have loaded an inappropriate driver for a display, it is possible that the system will crash when the driver is loaded in memory. In order to fix the problem, restart the system and choose F8 upon startup. This displays the Windows Advanced Startup Menu, where you will choose VGA mode. This will ensure that the video driver is not loaded (preventing the crash) so that you can then remove the driver through Device Manager.
- » **No image on the screen:** If you experience no image on the screen, ensure that the power is connected to the display, the power is on, and the computer is connected to the display. If you are connected to a projector and using a laptop, you may need to use the function keys to toggle your screen output to the projector.
- » **Overheat shutdown:** If you are experiencing a device that is shutting down, it could be due to overheating. You should take some time to clean the device, especially focusing on cleaning the dust away from air vents and fans on the device.
- » **Dead pixel:** A pixel on the screen that will not light up. It is a permanent black spot on your screen. You can use diagnostic programs to help detect and try to fix problems related to pixel display.
- » **Artifacts:** Visual artifacts are problems, or abnormality, in the display of information on the screen. This could happen as a result of hardware problems or driver issues.
- » **Color patterns incorrect:** If you are experiencing problems with the colors displayed on the system, check your color-correction settings, such as the brightness and contrast. This could also occur if the monitor is not connected properly.
- » **Dim image:** If you are experiencing a dim image or faded display, check the brightness settings. This can be found in your display driver options — or if you are using a laptop, check the power options. Check that the monitor is connected properly, as well.

- » **Flickering image:** If your display is flickering, there could be a weak connection to the display. Disconnect and reconnect the cable connecting the display to your system.
- » **Distorted image or geometry:** If you are having problems where the display is distorted, it could be your video driver or a bad video card. In order to fix the problem, you should try to replace the driver first and, if that does not work, try swapping out the video card.
- » **Discoloration (degaussing):** Older CRT monitors could experience discoloration from external magnetic fields. If you experience such discoloration, you can use a *degausser* to reduce the magnetic field and remove the discoloration.
- » **Burn-in:** This refers to a permanent discoloration of the monitor's display surface due to the prolonged display of non-moving images. CRT and earlier plasma displays are susceptible to screen burn-in; LCD displays can suffer from image persistence, but this can typically be cured by "exercising" the display. This "exercise" usually involves changing each pixel's state numerous times to "unstick" its persistent illumination state.
- » **Oversized images and icons:** This symptom is a clear indication of an incorrect screen resolution. If your monitor's native resolution is 1920 x 1080 pixels, then a 1024 x 768 resolution makes screen images and icons look enormous.
- » **BSOD:** Windows systems may experience the blue screen of death (BSOD) if the wrong video driver has been loaded or the driver has gone corrupt. If you experience regular blue screens, while restarting the system, choose F8. Then select VGA mode from the Advanced Startup Menu. Once Windows has loaded in VGA mode, remove the corrupt driver through Device Manager.

## ***Troubleshooting projectors and displays***

Projectors and other larger-format displays are popular in schools and businesses because they allow you to, well, present content to a group at once. As an IT professional working in such an environment, you will invariably be called upon to diagnose and resolve projector-related

problems. Some of these common symptoms and resolutions include the following:

- » **No power:** Look for an indicator LED on the projector. Refer to the operation manual for guidance on what indicator color codes mean. Oh, and make sure the unit is plugged in and switched on.
- » **No signal:** Verify you are using the proper input.
- » **Partial image:** Likely due to a resolution mismatch between the computer/television connected to the projector and the projector itself.

Keep in mind that some projectors and larger-format displays create a log file that tracks its operations. Look for multiple failure entries in the log file to help speed your troubleshooting/resolution time.

## *The Sound of Computers*

Another very popular output device is the sound card. As an output device, the *sound card* is responsible for sending sound data to the speakers, but can also be used as an input device by lining-in an external source to the card. For example, you could line-in a stereo system through your sound card and convert some old audio tapes to MP3 files.

The sound card contains a digital-to-audio converter (DAC) that converts the digital data from the computer into analog signals that create the sound. The sound card has a number of ports on the back that allow you to connect both output devices and input devices:

- » **Line-in:** This port is used to connect your CD player or stereo system and use it as a source for what the sound card plays. A great idea to get your old tapes to MP3 format!
- » **Mic:** Connect a microphone, which acts as a source for information being recorded.
- » **Headphones:** Connect your headphones.

- » **Line-out:** Just like you can connect your stereo to the computer via the Line-in port, you can also take sound on the computer and “line it out” to the stereo.

## *Types of sound cards*

You can find a number of different types of sound cards. The most popular interfaces for a sound card are as follows:

- » **Peripheral Component Interconnect Express (PCIe):** Today’s systems use PCIe sound cards that are Plug and Play and are inserted into the PCIe slots on the motherboard.
- » **USB:** More and more devices are found in USB format today, and sound cards are no different. You can also get a USB audio interface to connect to the USB ports on the system. In fact, many USB microphones have integrated audio interfaces.
- » **Integrated:** Some motherboards also have *integrated* sound cards, meaning that the motherboard has the sound card built in and you don’t need to purchase an additional card to install in the computer.

## *Installing a sound card*

Installing a sound card is no different than installing any other type of card. You first need to decide what type of card you want to use in your system (and then go buy one). With sound cards, you are most likely using a PCI card, but you may use a new PCIe slot.

Here’s how to install a sound card:

1. **Power-off and unplug the computer.**
2. **Open the case or side panel of the computer to access the expansion slots.**
3. **If you’re replacing a sound card, take out the old one.**

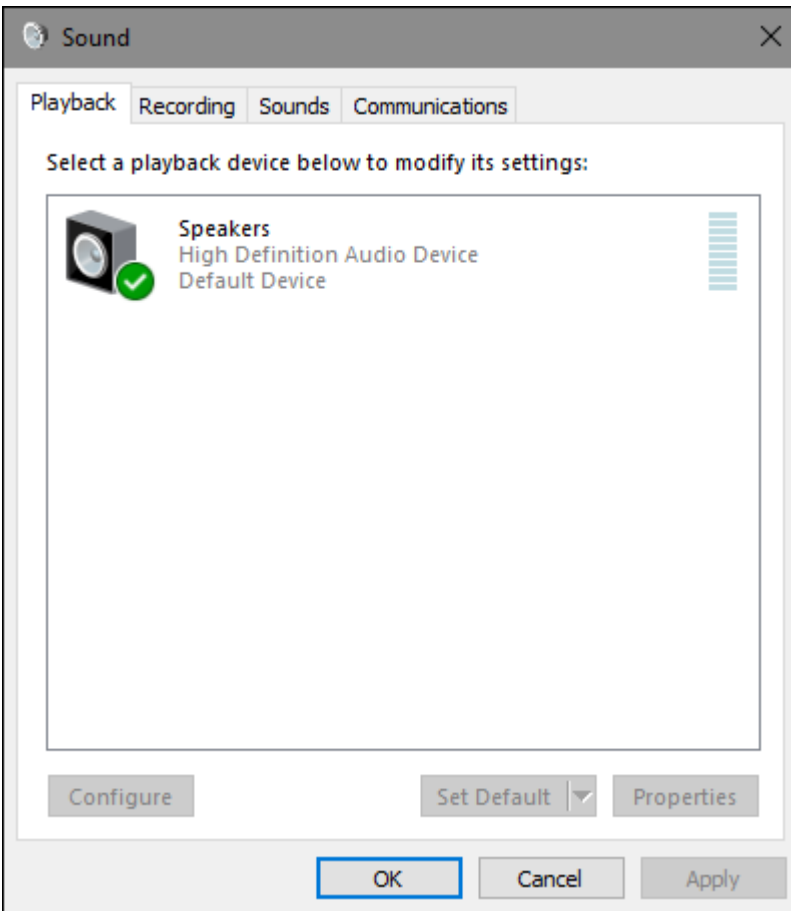
If the old sound card is integrated into the motherboard, you will not be able to remove it, and you might have to disable it in CMOS.

- 4. If this is the first sound card for the system, remove the blanking plate for the PCI or PCIe slot you wish to use.**
- 5. Insert the card into the slot until it fits firmly.**
- 6. Screw the sound card's plate into place to secure the card.**
- 7. Place the cover back on the computer and power-up the computer.**

Plug and Play should detect the device. After Plug and Play detects the sound card, it might prompt you for the driver. If so, supply the CD that came with the card. If you are not prompted for the driver and Windows did not load a driver, you might need to run the driver setup program from the CD that came with the card.

### ***Configuring a sound card***

After the driver is loaded for your sound card, you can configure the sound card by going to the Sound applet in the Windows Control Panel. To configure the sound card, choose Start, type sound, and select the Sound Control Panel result. This brings up the Sound Properties dialog box, as shown in [Figure 3-3](#).



**FIGURE 3-3:** Configuring sound settings in Windows 10.

The following list summarizes each tab and the types of settings to configure in the Sound Properties dialog box:

- » **Playback:** Set your speaker volume.
- » **Recording:** If you have a microphone, you can set recording levels and perform a sound check.
- » **Sounds:** Change your system sounds (alerts, startup and shutdown sounds, and so on).
- » **Communications:** Specify a preference as to how Windows automatically adjusts audio levels when you use the microphone.

## *Other Output Devices*



Video cards and sound cards are two of the most popular types of output devices found in systems today, but they are not the only types of output devices. This section overviews some of the other types of output devices found in computer systems:

- » **Multimedia cards:** Not really an output device, but when it comes to multimedia, video and sound files have to be stored somewhere.
- » **Display devices:** Display devices such as monitors and projectors are common output devices. Be sure to know the quality of your display device when purchasing it. Look at the resolution supported, contrast ratio, and lumens to determine the best quality display device.
- » **Printers:** Another example of an output device is a printer. This output device is so important that I have dedicated its own chapter to it. Check out Book 3, [Chapter 4](#) to learn about installing and troubleshooting printers.
- » **Speakers:** The sound card in the computer is typically connected to a set of speakers that are designed to output the sound of the computer.
- » **I/O devices:** Any number of input/output (I/O) devices may be connected to your system. These devices (such as printers, scanners, and fax devices) can connect to your system in any form, such as SCSI, serial, or even parallel. Here is a summary of some of the technologies used with I/O devices:
  - *SCSI:* This legacy technology supports *daisy-chaining* (having one device connect to the next). To connect a SCSI device to your system, you need a SCSI card, and you also need to ensure that you assign unique IDs to each device and terminate both ends of the SCSI bus. Typically, storage devices such as drives, CD-ROMs, and tapes appear as SCSI devices.
  - *Serial:* Some I/O devices are serial devices that connect to the serial port of the computer. An example of an I/O device that may connect to the serial port is a modem.

## Getting an A+

In this chapter, you find out about the two major types of output devices found on systems today: the video card and the sound card. The following summarizes some key points about video and sound cards:

- » The video card converts digital data from the computer into analog data that is used by older monitors to create the display.
- » VGA supports 16 colors at a resolution of 640 x 480.
- » Super VGA supports 16 million colors at a resolution of 1280 x 1024.
- » AGP cards were once a popular form for video cards, but you rarely see this interface nowadays.
- » PCIe cards are the popular form for video cards today, and sound cards are implemented as PCI cards.
- » CRT monitors use an electron gun to stimulate the phosphor-covered screen and make it glow.

## *Prep Test*

- 1. Modern sound cards are connected to the system using which of the following? (Select two.)**
  - (A) AGP
  - (B) ISA
  - (C) PCIe
  - (D) USB
  
- 2. Which video standard supports 16 colors at 640 x 480 resolution?**
  - (A) EGA
  - (B) VGA
  - (C) SVGA
  - (D) CGA
  
- 3. What type of display is found on laptops?**

- (A) CRT
- (B) LCD
- (C) RCT
- (D) USB

**4. Which video standard supports only four colors?**

- (A) EGA
- (B) VGA
- (C) SVGA
- (D) CGA

**5. Which type of display uses an electron gun?**

- (A) CRT
- (B) LCD
- (C) RCT
- (D) AGP

**6. Which video standard supports 16 million colors at 640 x 480 resolution?**

- (A) EGA
- (B) VGA
- (C) SVGA
- (D) CGA

**7. Which video characteristic represents the variance between brightnesses supported by the display?**

- (A) Resolution
- (B) Contrast ratio
- (C) Color support
- (D) Refresh rate

# Answers

1. **C, D.** Older sound cards were implemented as ISA cards, and newer sound cards connect using either PCIe (for internal cards) or USB (for external interfaces). See “[Installing a sound card.](#)”
2. **B.** VGA supports 16 colors at 640 x 480 resolution. Check out “[Looking at the video standards.](#)”
3. **B.** LCDs are found on laptops but are also used with desktop computers today. Take a look at “[LCD.](#)”
4. **D.** CGA supports only four colors. Peek at “[Looking at the video standards.](#)”
5. **A.** A CRT monitor uses an electron gun to light phosphors on the screen. Look over “[Cathode ray tube \(CRT\).](#)”
6. **C.** SVGA is the video standard used today, and it supports 16 million colors. Study “[Looking at the video standards.](#)”
7. **B.** Contrast ratio, such as 3000:1, indicates the variance in brightness between bright colors and dark colors “[Evaluating display features.](#)”

# Chapter 4

## Managing Printers

---

### IN THIS CHAPTER

- » Identifying paper feeder mechanisms
  - » Understanding types of printers
  - » Identifying printer connections
  - » Identifying common printer problems
  - » Understanding preventive maintenance and safety precautions
- 

In today's business world, maintaining a printing environment is one of the most time-consuming parts of managing a network. For a supposedly paperless era, we seem to spend a lot of time troubleshooting why a printer won't print!



**FOR THE  
EXAM**

This chapter introduces you to the different types of printers and describes how each type of printer works, which is important for the A+ certification exams. From an exam point of view, be sure you are extremely comfortable with the parts of a laser printer and the six phases of the laser printer's print process — you are guaranteed to get some questions on it!

Be sure to also go over the troubleshooting sections. I think that most people simply skim over this topic area, but you will be presented with some common problems on the A+ exams, and you are responsible for identifying which component of the printer is causing the problem. Be sure to spend some time on this chapter!

# *Learning about Paper Feeder Mechanisms*

A printer is useless without something to print on, so how the paper gets into a printer seems like a perfect place to start the discussion. The paper enters the printer through a *feeder*, technically a *paper feeder mechanism*. The paper feeder mechanism pulls or pushes the paper into the printer. The two types of paper feeder mechanisms are

- » Continuous form feed
- » Friction-feed

The following sections take a close look at both of these types of paper feeders.

## *Continuous form feeders*

Continuous form feed printers use a continuous sheet of 8.5"- or 14"-wide paper. The continuous sheet feeds through the printer, and then the sheets are separated after the print operation. The pages are usually perforated to make this easier and to maintain a consistent size.

The paper has holes along both sides that fit over the sprockets located on the feeder wheel. When the wheel turns, it feeds the paper into the printer. The holes are torn off the paper after the printout is complete.

And, yes, printers still use this type of feeder mechanism. One common use is for printing company paychecks. Blank checks are connected as a continuous sheet of paper and fed into the printer. After a check prints, it moves out of the printer, and the next check is fed in. After all the checks have printed, the accountant then separates each check for distribution to the employees.

Dot matrix printers are an example of a continuous form feed printer.

## *Friction feeders*

The most popular type of printers are friction feed printers, which use two rollers that pick up sheets of paper from a paper tray and feed them through the printer.

With friction feed printers, many different types of rollers are used throughout the print process. The rollers that pick the paper from the tray are “pickup” rollers, but other rollers pass the paper through the different parts of the printer.

Laser printers, photocopiers, and fax machines are friction feed printers.

## *Understanding Types of Printers*



FOR THE  
EXAM

The different types of printers in today’s busy world of computing are laser, inkjet, dot matrix, thermal, and virtual. You need to be familiar with each type for the A+ exams.

### *Laser printers*

The laser printer — also known as a *page printer* because it prints one page at a time — is the most popular type of printer because it is fast and reliable, and offers the best-quality printout of the three types of printers.

A laser printer gets its name because it uses a laser beam in the printing process. A laser printer, shown in [Figure 4-1](#), is also the most expensive type of printer because of its high-cost components such as the laser.



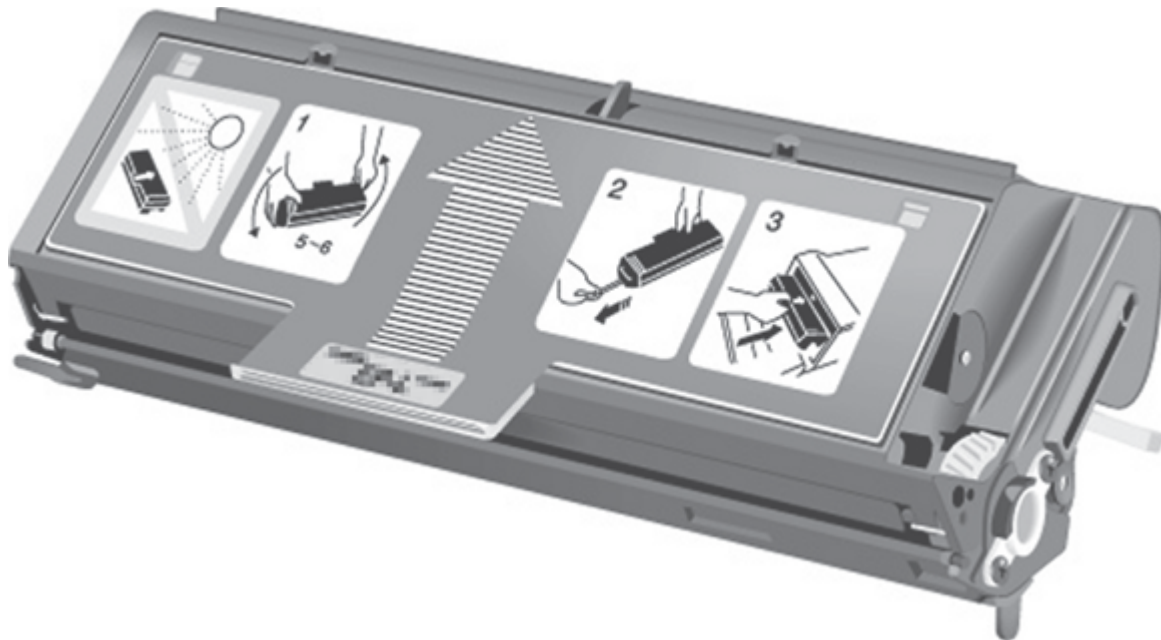
**FIGURE 4-1:** Looking at a laser printer.

Many parts work together to make the laser printer and its printing process run smoothly:

- » **Paper feeder mechanism:** Laser printers use a set of *pickup rollers* to grab the paper from the paper tray and feed it into the printer.
- » **Paper transport path:** Rollers are used throughout the print process so that the paper can continue to move through the printer.
  - *Registration rollers* move the paper.
  - *Fuser rollers*, also known as the fuser assembly, melt the toner onto the paper.
  - *Exit rollers* guide the paper out of the printer.



- » **Toner cartridge:** The toner cartridge (shown in [Figure 4-2](#)) contains the replaceable components of the printing process. It contains three core components:
- *The toner* is electrically charged material made of pigment (to give it its color) and plastic (so it can be melted to the page) that is attracted to the paper to create the printout.
  - *The print drum*, also known as the imaging drum, holds an electromagnetic charge when exposed to the laser. That charge then attracts the toner to the page.
  - *The cleaning blade* cleans excess toner off the drum after the print process has completed.
- » **Power supply:** The power supply in the printer is responsible for converting AC from the wall outlet into DC that charges the primary corona wire and transfer corona wire as well as with other components of the printer.
- » **Primary corona wire:** The primary corona wire applies the initial – 600V charge to the drum.
- » **Transfer corona wire:** The transfer corona wire gives the paper a positive electrical charge that is used to attract the toner to the paper.

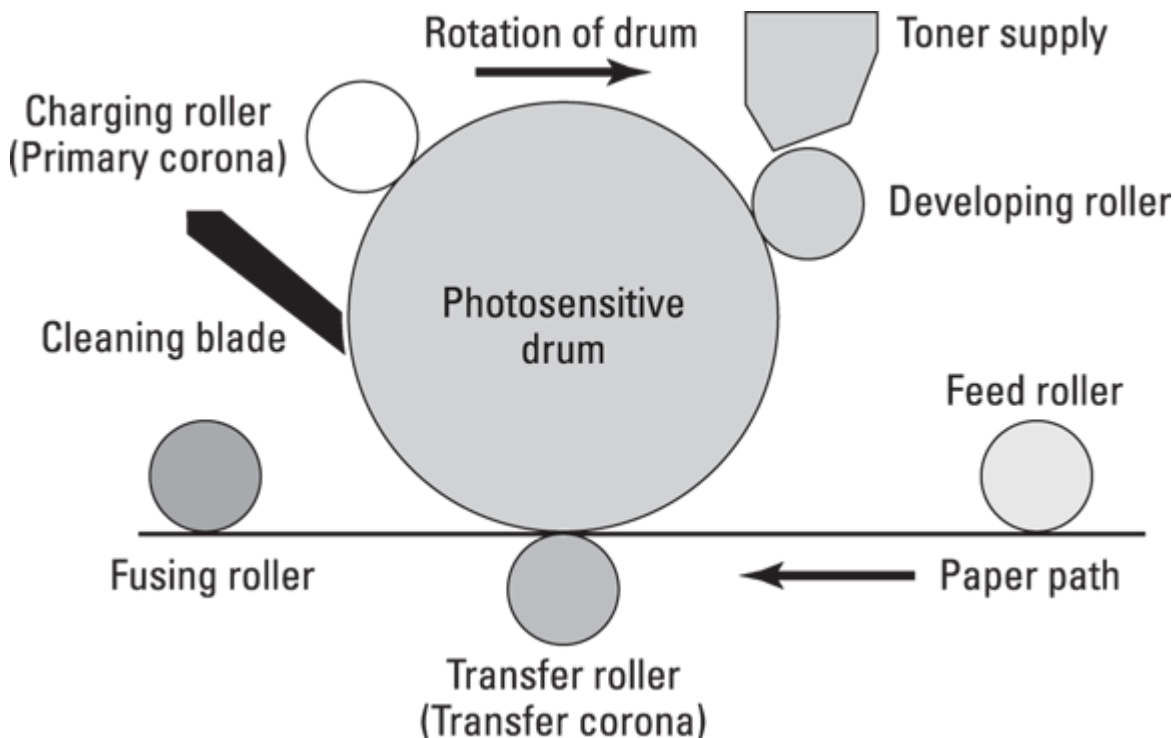


**FIGURE 4-2:** A toner cartridge found in laser printers.

Each component of the laser printer is used to perform the print operation. The process used to perform the printer operation is the *laser printing process*.

### ***The laser printing process***

The laser printing process has six phases, and you are required to know them for the A+ exams. Knowing the process is the basis for effective printer support and is essential for passing the A+ exams. The six phases of the laser printing process are conditioning, writing, developing, transferring, fusing, and cleaning. As you read the following sections, identify where each step occurs in the schematic in [Figure 4-3](#).



**FIGURE 4-3:** Identifying the laser printing process.

#### ***1. CHARGING THE DRUM (CONDITIONING)***

This phase is often known as the conditioning or charging phase. When the printer receives a command from the computer's operating system to begin the print process, the primary corona wire applies a  $-600\text{V}$  charge

to the photosensitive drum, also known as the *print drum*. This charge is one reason why a printer requires a high-voltage power supply.

## **2. EXPOSING THE DRUM (WRITING)**

This phase is often referred to as the exposing or writing phase. After the drum has the  $-600\text{V}$  charge, a laser beam is used to hit areas on the drum to create the image to be printed. In the areas on the drum that the laser touches, the charge changes from  $-600\text{V}$  to approximately  $-100\text{V}$ .

Recognize that the areas exposed to the laser beam are more positively charged.

## **3. DEVELOPING THE IMAGE (DEVELOPING)**

After the image is created on the photosensitive drum, toner is used to develop the image on the drum. Alongside the print drum is the developing roller. The developing roller has a  $-600\text{V}$  charge, which attracts the toner from the toner reservoir to the developing roller.

Because the print drum and the developing roller are both charged to  $-600\text{V}$  (except for the areas of the print drum previously exposed to laser light), the toner from the developing roller is attracted to the  $-100\text{V}$  charged areas of the print drum. This entire concept is based on the “opposites attract” principle. Although both the drum and the roller are both negatively charged,  $-100\text{V}$  is more positive than  $-600\text{V}$ , so the toner on the  $-600\text{V}$  roller is attracted to  $-100\text{V}$  areas on the drum. Now that the print drum has toner on only the areas of  $-100\text{V}$  charge, the image is ready for transfer to paper.

## **4. TRANSFERRING THE IMAGE (TRANSFERRING)**

After the toner is on the print drum, the feed rollers (also known as the registration rollers) feed the paper into the printer and over the transfer corona wire. The *transfer corona wire*, also known as the *secondary corona wire*, applies a very strong positive charge of  $+600\text{V}$  to the paper. The purpose of such a strong charge to the paper is to ensure that the toner will be attracted from the  $-100\text{V}$  areas of the drum to the paper. This, too, is based on the rule that opposites attract!

The paper continues to move through the assembly, and passes over the drum to attract the toner from the drum to the paper.

## 5. FUSING THE IMAGE (FUSING)

After the paper moves past the print drum and holds the toner, the paper then moves through the fusing rollers, which melt the toner to the paper. The fusing rollers are needed because the only thing holding the toner to the paper at this point is a positive electric charge. During the fusing phase, the paper moves between a heated, Teflon-coated roller and a rubber roller, which melt the toner in place. The paper is then ejected from the printer.

## 6. CLEANING UP THE MESS (CLEANING)

After the printing has completed, any excess toner that remains on the print drum needs to be cleaned off. That's the purpose of this last phase — the cleaning phase. A cleaning blade scrapes any leftover toner off the print drum and into a holding tray to prepare the drum for the next print operation.



FOR THE  
EXAM

The A+ certification exams focus on laser printers when it comes to asking questions about printers. Be familiar with dot matrix and inkjet printers, but most of all, be sure that you are comfortable with laser printers and the laser printing process.



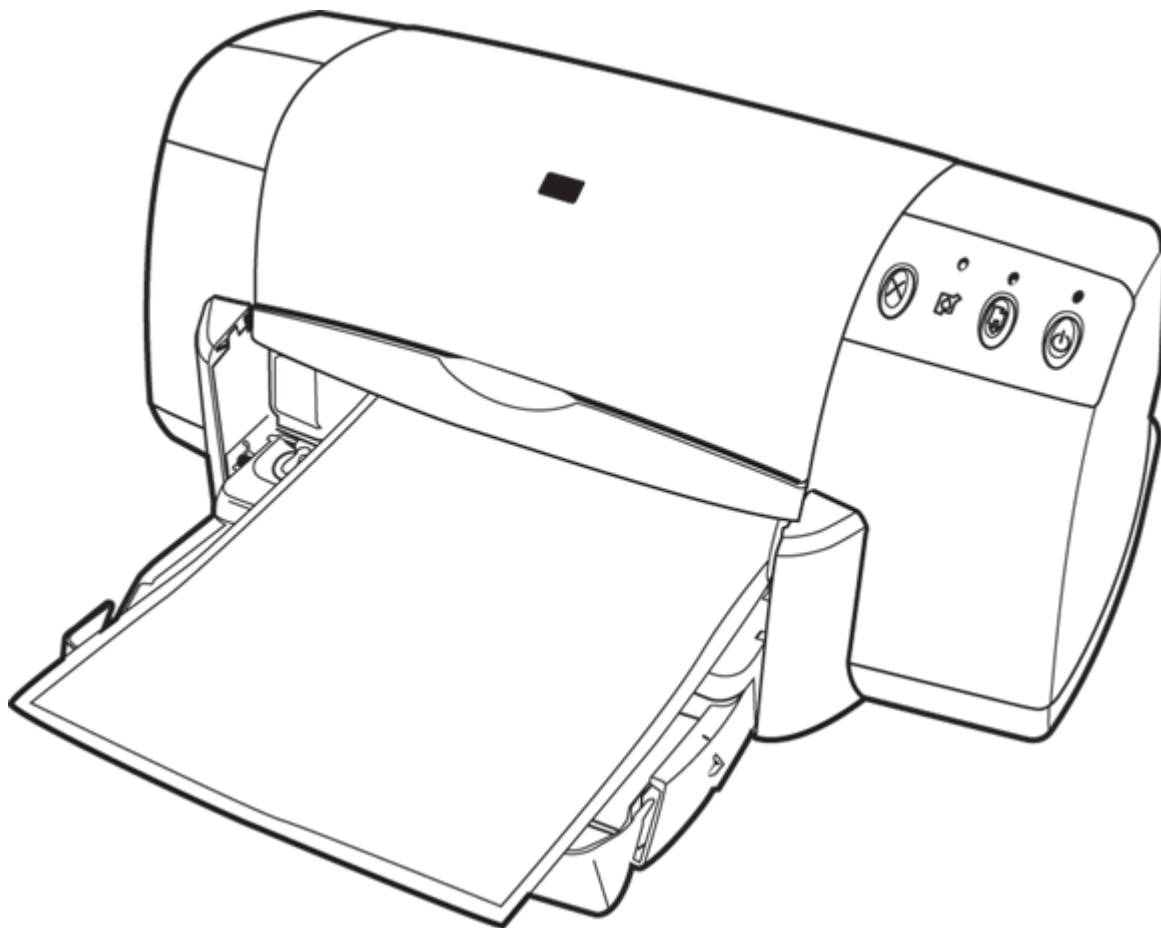
ON THE  
WEB

Lab 4-1 will help you identify parts of the laser printer. You will need a laser printer available to perform this lab. Lab 4-1 can be found on the companion website at

[www.dummies.com/go/aplusaio](http://www.dummies.com/go/aplusaio).

## *Inkjet printers*

Inkjet printers (see [Figure 4-4](#)) offer the next highest level of print quality and are relatively cheap compared to laser printers. Inkjet printers are great for home use or small office environments that don't have large print jobs.



**FIGURE 4-4:** An inkjet printer.

Inkjet printers don't use toner like a laser printer; instead, they use ink cartridges. The ink cartridge contains all the working elements needed to get an image from the computer onto a sheet of paper. It contains compartments of ink, each sealed with a metal plate to prevent ink leakage. Each compartment has a tiny pinhole from which the ink is sprayed from the cartridge onto the paper.

What's interesting about ink cartridges is that each has its own integrated print head. The printer's paper roller, feeder assembly, carriage, and belt are similar to these parts on other printer types. Nowadays duplexing (the capability for the printer to produce two-sided output) is pretty standard on most mid-level inkjet print devices.

When the printer receives the command from the computer to print an image, the printer starts the print process by applying an electrical charge to the heating elements that are in the ink reservoir. The charge heats the

heating elements, which cause the ink to vaporize. The vaporized ink creates pressure and is forced out the pinhole, creating a tiny bubble that hits the paper.

Color inkjet printers are very popular today because of the increased popularity of digital cameras. Color inkjet printers can require two cartridges: one for black ink and one for the colors (cyan, yellow, and magenta). Most inkjet printers today have cartridges that bundle the black ink with the other colors. These cartridges are called *CYMK* (C for cyan, Y for yellow, M for magenta, and K for black).

Some printer manufacturers offer individual cartridges for each color. The benefit of these printers is that if you run out of one color, you simply need to buy only the cartridge that contains that color, not all the colors.

One thing to keep in mind is the print cartridges/print heads fall out of alignment on a regular basis. Therefore, you should make a habit of recalibrating the print output for any inkjet printers that you maintain. You should find that calibration utilities are built into the print device's management software.



**TIP**

When it is time to replace a spent ink cartridge, take the old cartridge with you to the store so that you know which cartridge type to buy. Some office supply stores can recycle your old cartridges, sometimes even offering a discount when you turn in your old cartridges. If you do not want to take the old cartridge with you to the store, make sure you know the make and model of the printer that you are buying the cartridge for.

## ***Multifunction printers***

Multifunction printers are laser or inkjet printers that incorporate other functions besides printing into a single hardware device. Typically, multifunction printers include scan and fax functionality, and are often WiFi-enabled both for infrastructure and ad-hoc wireless networks. And any multifunction printer worth its salt, like the HP OfficeJet Pro 6830

that I use in my office, support advanced printing features like duplex (two-sided) printing and collation.

Many business-class multifunction laser or inkjet printers include an internal hard disk drive that the device uses to cache incoming print jobs. This hard drive caching allows the printer to service more print jobs per unit time than it could by using its much-more limited internal RAM.

### ***Dot matrix printers***

Dot matrix printers are considered *impact* printers because they physically strike an inked ribbon with a metal pin to put characters on paper. A dot matrix printer fires off rows of pins that strike the ribbon in patterns to create the image or characters that need to be printed. Each pin — a *solenoid* — is wrapped in a coiled wire held in place with a spring and small magnet. When a solenoid is needed to help create the image by striking the ribbon, an electrical charge is sent down the coil wire that surrounds the solenoid. The electrical charge around the wire causes the magnetic field from the magnet to be lost, resulting in the pin firing against the ribbon.

The solenoids are contained in the *print head*, which moves across the paper printing one line of dots at a time. Originally, dot matrix printers used only nine pins in the print head. The 9-pin dot matrix printers were known as *draft-quality* printers and were later replaced by 17- and even 24-pin dot matrix printers. The quality of the 24-pin dot matrix was much better than that of the 9-pin because the greater number of dots creates a finer image.

### ***Thermal printers***

For the A+ exams, you simply need to focus on laser, dot matrix, and inkjet printers. Another type of printer you might encounter, though, is a thermal printer, which creates printouts on special paper by heating a stylus pen located on a print head. The pen then causes a chemical reaction on the special paper that is sensitive to heat.

### ***Virtual and cloud-based printers***

A virtual printer is a non-physical print device that exists on your local system. What do I mean, you ask? Well, I'm here to tell you that every time you use the Portable Document Format (PDF) printer with Adobe Acrobat, or the Microsoft XML Paper Specification (XPS) printer that is included with the Office productivity suite, you're in fact using a virtual printer. A virtual printer exists entirely in software, and its sole purpose is to "print" output to a document or image file.

Printing to a file or image is a great benefit to individuals and businesses who covet the so-called "paperless office." By using virtual printers you not only contribute to the environment by consuming less paper, but you also save money on otherwise expensive consumables like inkjet and toner cartridges.

By contrast, a cloud printer is a virtual printer whose device drivers and managed, well, in the cloud. Apple AirPrint and Google Cloud Print are two cloud printing technologies whose goal is to make it easier for you and others to print output from any print device without having to go through the trouble of installing a device driver.

Here's how cloud-based printing works: You connect your AirPrint- or Cloud Print-enabled printer to your WiFi network. Next, you choose the Print function from any application running on another host from the same WiFi network. The cloud printer should be available, and your print job will go through despite your not having manually loaded device drivers and/or configuration utilities. Pretty neat!

For those of you who are concerned about security (and that should be all of you): As long as you have authentication enabled on your WiFi network, your cloud-based print queues should be safe from unauthorized parties. That said, the data privacy aspect is enough to scare many individuals and businesses away from any technology that mentions "cloud" in its name.

### ***3D printers***

A 3D printer allows you to make three-dimensional solid objects from a digital blueprint file. The creation of the objects takes place by the printer



laying down layer after layer of plastic filament until you have the completed object.

3D printers have a number of practical applications beyond the “maker” joy: product prototyping, scale models, proof of concept, and so forth.

### *Common parts on the printer*

Whether you are using a laser printer, inkjet printer, or dot matrix printer, some parts are common to each of the printer types, although how they physically print is different. The following are some common elements to each printer type:

- » **Print head:** The print head is responsible for the printing. With inkjets, the print head contains the nozzles that shoot out the ink, while a dot matrix print head contains the pins that shoot out.
- » **Heating element:** The “thermal” in “thermal printer” denotes the necessity of a heating element. The element heats the ink that the print head affixes to your paper. Incidentally, thermal printers require special thermal paper, so stock up!
- » **Feeder:** The feed assembly is responsible for picking up the paper from the paper tray and feeding the paper into the printer.
- » **Roller:** Many printers have rollers to move the paper through the printer.
- » **Duplexing assembly:** The duplexing assembly is responsible for allowing automatic printing on both sides of the page. The duplex assembly can be added to many printers to obtain automatic duplexing capabilities.
- » **Carriage and belt:** The carriage-and-belt system is the part of the printer that moves the print head back and forth across the page.
- » **Paper tray:** The paper tray holds the paper while it is waiting to be picked up and sent through the printer.

# *Viewing Types of Printer Connections and Configurations*

In this section, you find out how printers are connected to computer systems in order to communicate. The following are the most popular methods to connect a printer to a computer:

- » Network connections (Ethernet)
- » Wireless
- » Universal Serial Bus (USB)
- » Infrared

## *Network cable connections (Ethernet)*

Network-based printers have built-in network cards that allow the printer to connect directly to the network. The printer runs the TCP/IP protocol and is assigned an IP address so that it can participate on the network.

You can assign the IP address to the printer through the menu system of the printer. After the IP address is assigned, you can typically manage the settings on the printer through a web browser by typing the IP address of the network printer in the address line of the browser.

Advantages of using a network-based printer are

- » **The network printer is available all the time.** Network-based printers are connected directly to the network, so they don't rely on a computer being powered-on to communicate with the network.
- » **Dedicated print servers are not required.** A network printer can be accessed from anywhere in the network, and you don't need to have a server to print to it. You may print to the network-based printer from the client computer directly.

Today's network printers also support network connectivity via wireless network cards. This gives the benefit of not needing a network jack close

by to connect the printer to the network. You can read more about network cards and wireless networking in [Book 8](#).

## *Wireless connections*

Many printers today allow you to connect the printer to the network using a wireless network connection. Many modern printers support 802.11x wireless networking capabilities. You can configure an IP address on the wireless printer (usually through software or through the menu system on the printer) and then connect to that wireless printer from any wireless or wired network client on the network.



**TIP**

Note that 802.11x refers to any of the IEEE 802.11 WiFi protocols. The  $x$  is used in an algebraic way; namely, to serve as a variable. The  $x$  could stand for  $a$ ,  $b$ ,  $g$ ,  $n$ , or  $ac$ .

Not only do printers support 802.11x printing capabilities, but many printers also support Bluetooth networking capabilities that allow you to connect to the printer over short distances. You can find out more about wireless technologies by checking out Book 8, [Chapter 2](#).

## *Universal Serial Bus (USB)*

Most printers today purchased for home or small offices are USB printers that connect to the computer via a USB port (go figure). [Figure 4-5](#) shows a USB connection.



**FIGURE 4-5:** A USB connector is a popular method today to connect printers to computers.

USB has a number of benefits, including the fact that it is a Plug and Play technology (you can plug in the device without shutting down the system). USB 1.1 has a transfer rate of 12 Mbps, USB 2.0 has a transfer rate of 480 Mbps, and USB 3.0 has a transfer rate of 5 Gbps!



**FOR THE  
EXAM**

For reference, the following are some key points to remember about USB:

- » It is Plug and Play.
- » You may connect 127 devices to a USB chain.
- » You don't need to configure ports, IRQs, or DMA channels for each device.

- » USB 2.0 has a transfer rate of 480 Mbps, while USB 3.0 has a transfer rate of 5 Gbps.

To find out more about USB ports, check out Book 2, [Chapter 1](#).



ON THE  
WEB

Lab 4-2 will give you the opportunity to practice connecting a USB print device to your computer. Lab 4-2 can be found on the companion website at [www.dummies.com/go/aplusaio](http://www.dummies.com/go/aplusaio).

## *Infrared*

Connecting your printer to a system by using infrared technology lets your computer communicate wirelessly with the printer in much the same way you use a TV remote to change channels without getting off the sofa. The infrared signal sent from the computer to the printer is carried as a beam of light, instructing the printer what to print.

To use an infrared printer, you need both an infrared transmitter/receiver connected to your computer and an infrared printer.

The three different types of infrared devices are

- » **Reflective infrared:** Transmitters send the signal to a central unit, which then redirects the commands to the printer. This allows a number of users to print to a single printer at one time.
- » **Line-of-sight infrared:** With line-of-sight, the printer's receiver must be in a direct line-of-site with the computer's transmitter. If there is a break in the line-of-site, communication is lost.
- » **Scatter infrared:** Scatter infrared allows the signal to bounce off walls or ceilings (or even people) all the way to the printer's receiver. The benefit is that you don't lose communication like you do with line-of-sight. However, scatter infrared has limited range and transmission speeds.

## *FireWire and SCSI*

You might also find printers that connect to a system via FireWire or SCSI connections. FireWire has two versions: 400 Mbps and 800 Mbps. FireWire 800 is also known as FireWire 1394b.

SCSI is another common type of printer device that you might come across with Macintosh systems. Most PC-based systems don't use SCSI printers, although it is possible. For more information on SCSI devices, check out Book 2, [Chapter 5](#).

### *Hardware print server*

In environments where a large number of print requests are happening on the network, the company may invest in a hardware print server as opposed to sharing the printer off a Windows system.

The benefit of a dedicated hardware print server is speed. Using a Windows system as a print server usually means the system is used for other tasks as well. The other tasks will slow down the printing environment as they use up the resources on the system.

## *Upgrading Printer Hardware*

Printers aren't nearly as upgradeable as computers. There are only a few items that may need upgrading on a printer:

- » Printer memory
- » Disk space on larger printers
- » Firmware updates

I discuss these upgrades in the following sections.

### *Upgrading memory*

A printer uses memory to store the information to be printed, so the more memory a printer has, the larger the print documents it can store. If you ever receive an insufficient memory message when printing a large document, your printer probably doesn't have enough memory. As a work-around, install more memory for the printer.

## *Adding a disk drive*

On larger printers, you can upgrade their hard disk or memory. The additional hard drive or RAM can store information used by the printer; for example, you might want to install some fonts on the printer, or you could have a print queue stored on the actual print device and use the hard drive to store the queued documents.

## *Upgrading the firmware*

You might also need to update the firmware on the printer. Firmware, which dictates the capabilities of the printer, is similar to the BIOS of a computer. Actually, it is so similar that you upgrade the firmware in a similar way as upgrading a BIOS. Start by downloading the firmware update from the manufacturer's website. This update is usually in the form of a self-extracting executable. Then double-click the executable to run the update.



**TIP**

Make sure that the printer is connected and powered-on when the update runs because the update program needs to rewrite the printer firmware within the physical printer.

## *Installing a Printer in Windows*

After you connect the printer to the computer, typically with a parallel or USB connection, you then need to install the “printer” into Windows. Windows uses the term *printer* to describe the software interface (the printer driver) used to communicate with the print device. This software interface is represented as the icon that displays in the Printers folders — the icon that you right-click to change the settings for the corresponding print device. Microsoft refers to the *printer* as the icon found in Windows, and the *print device* as the piece of hardware connected to the computer. I use these terms when discussing how you manage a printer in Windows.

## *Installing a printer*

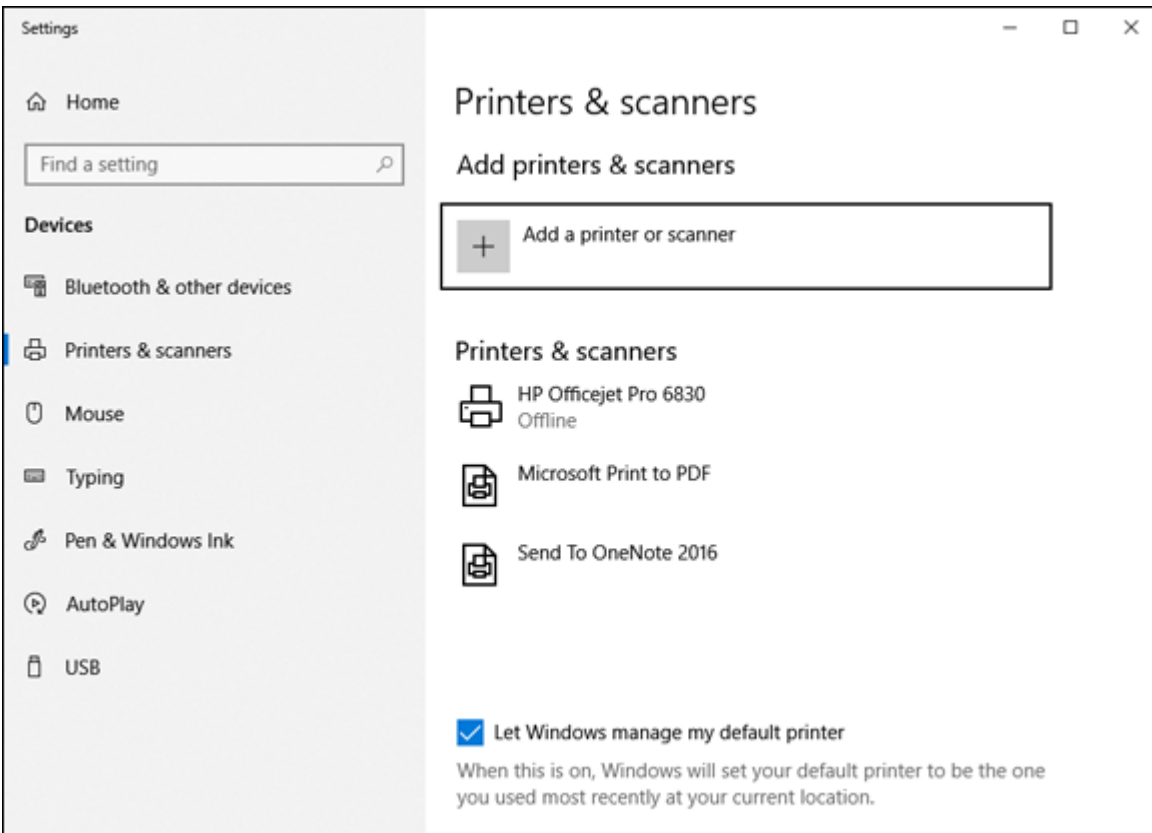
When you connect a USB print device to a Windows computer, Plug and Play kicks in and detects the hardware. If Windows has a driver for the print device, it loads that driver automatically; if it doesn't, it prompts you for the driver disk. After you supply the driver disk, the printer is installed, and you are off to the races!

For the following example, you'll install a local printer in Windows 10. Follow these steps:

1. **Open Start, type printer, and click the Printers & Scanners search result.**
2. **In the Printers & Scanners settings panel, click Add a printer or scanner (as shown in [Figure 4-6](#)).**
3. **In the Printers folder that opens, click the Add Printer button in the toolbar of the window.**
4. **If Plug and Play detects the printer, click its icon to let Windows provide a device driver.**  
You will also see a list of network printers if your systems administrator shared them with you.
5. **If Plug and Play fails to detect the printer, click “The printer that I want isn't listed” and follow the instructions.**

You can then point Windows to printer driver files that you might have downloaded from the manufacturer's website, or run the built-in troubleshooter.





**FIGURE 4-6:** Installing a local printer in Windows 10.

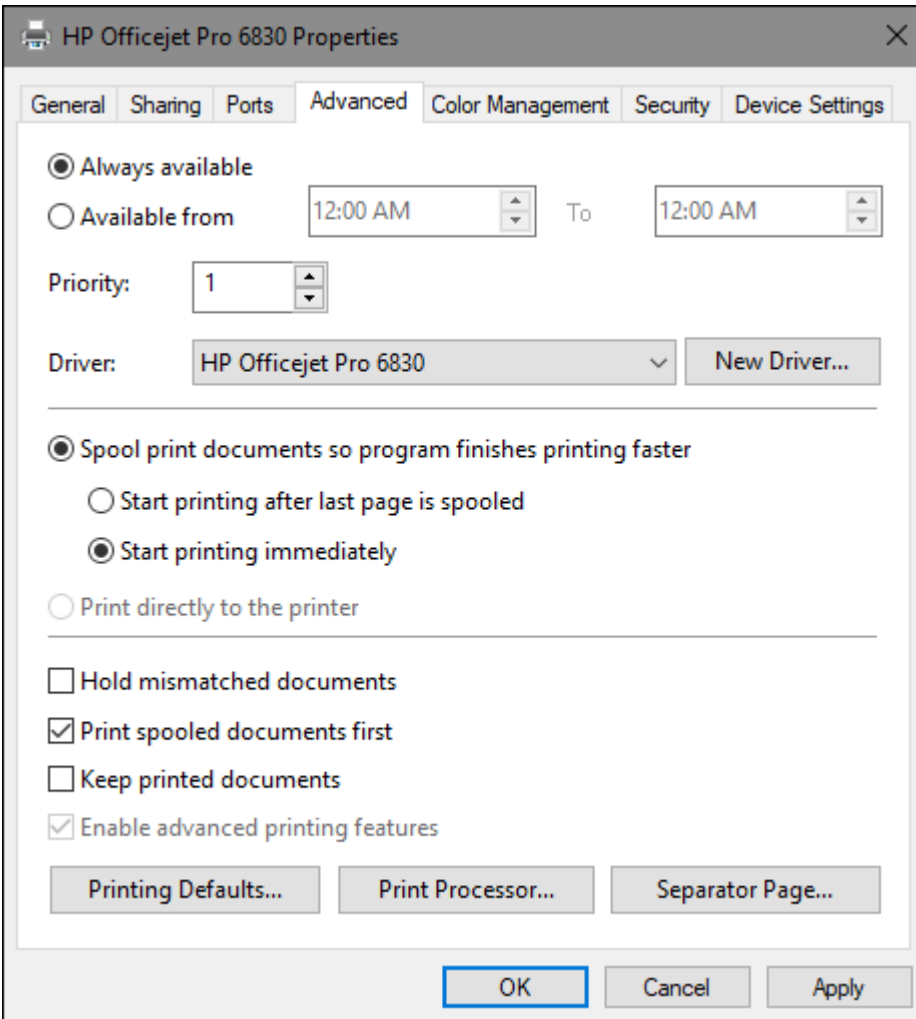
## *Configuring a printer*

After the printer is installed, you might want to configure it. To configure a printer in Windows 10, open the Printers & Scanners settings panel, select the printer, and click Manage. Next, click Printer properties, and the printer's Properties dialog box opens. The following is a list of popular printer settings that might need changed, depending on how you want to use the printer:

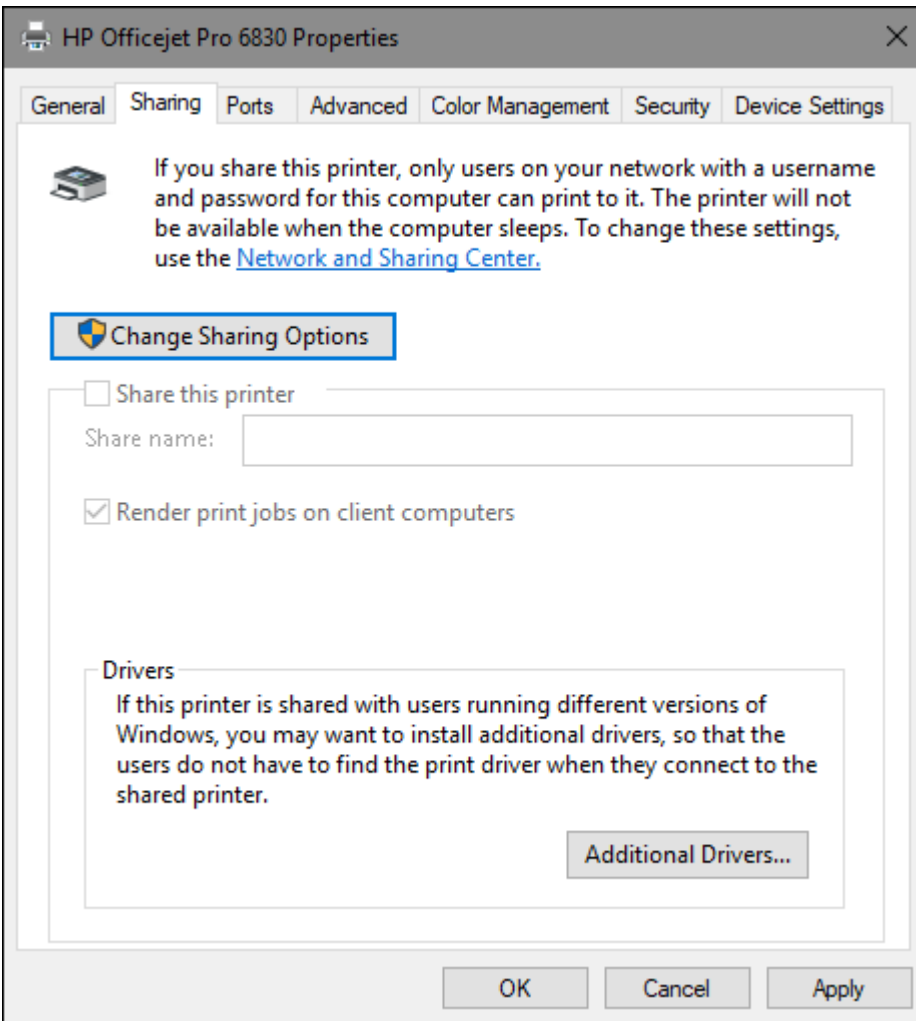
- » **Priority:** If a group of users needs a higher priority on a network print device, you could install two printers to refer to the same print device. After you have both printers installed, set the priority of one of the printers higher than the other — anyone's print jobs sent to that printer will have a higher priority on the print device. You can set the priority of a printer on the Advanced tab of the printer's Properties dialog box (shown in [Figure 4-7](#)).

- » **Schedule:** If you have a group of users that should be printing only at certain hours, you could set the schedule of the printer so that it can print only during those times. The user can send print jobs to the printer, and the printer will queue the job, or store it, until the scheduled time. At the scheduled time, it will then print the job. The schedule option can also be seen in [Figure 4-7](#).
- » **Spool settings:** In Windows, when a user chooses to print a document, the print job creates a temporary file on the disk for the document being printed. After the file is stored on disk, the user gets control of the application, and the system sends the temporary file to the print device to be printed. While the temporary file is sent to the print device, the user gets to use his or her program again. This is sometimes referred to as *background printing* — where the user thinks the print job has been sent, but the print job is actually being sent while the user continues using the computer. The purpose of this process, called *spooling*, is so that users can continue using the computer instead of waiting for the 20 pages to actually get sent to the print device. Because temporary files are stored on the disk when spooling is enabled (which is the default with all Windows printers), if you don't have the hard disk space on your computer to store the temporary files, you won't be able to print. If you get a spooling error, you may turn off spooling by choosing Print Directly to the Printer on the Advanced tab. Again, you can see this option in [Figure 4-7](#).
- » **Driver:** If the printer driver becomes corrupted, you might want to change the driver. Go to the Advanced tab of the printer's Properties dialog box and click the New Driver button. You will then be asked for the make and model of the printer.
- » **Print Test Page:** If you run into trouble with a printer, you might want to print a test page. On the General tab of the Properties dialog box of a printer, click Print Test Page. Printing a test page will help you determine whether you are having a problem with the printer or a problem with an application. For example, if you cannot print from Microsoft Word but you can print a test page, that indicates that a setting in Microsoft Word is causing the printing problems.

» **Sharing:** If you are in a networked environment, you can share the printer so that other users on the network can print to it from their computers. To share the printer, go to the properties of the printer and click the Sharing tab. Select the Share This Printer option and give the printer a share name, as shown in [Figure 4-8](#).



**FIGURE 4-7:** The priority setting and the scheduling option on a printer.



**FIGURE 4-8:** Sharing a printer.

The following steps show how to change your printer properties in Windows 10:

1. **Click Start, type printer, and select the Printers & Scanners result.**
2. **In Printers & Scanners settings panel, select the printer you want to configure.**
3. **Click Manage.**

### *Connecting to the shared printer*

When you have shared a printer, users need to install a printer on their systems that points to the shared printer on the network. Users who install

a printer that refers to a shared printer on the network are installing a network printer. A *network printer* refers to a shared printer on the network by what is known as a *universal naming convention (UNC)* path. A UNC path always has the syntax of

```
\\computername\sharename
```

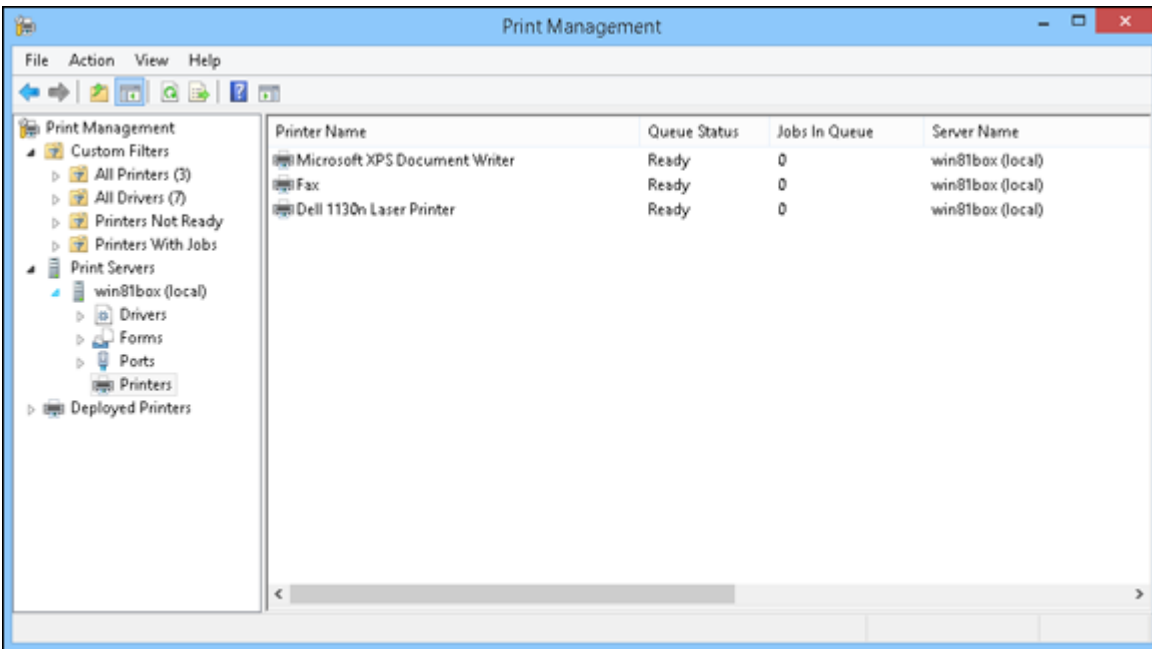
The `computername` parameter is the name of the computer that has the printer shared, and the `sharename` parameter is the name the printer has been shared as. For example, assume you have a system with a computer name of `WORKSTATION1`, which has a printer shared as `HP`. To connect to this printer, you would type `\\workstation1\hp` from the `Run` command or when installing the network printer.

To install a network printer in Windows 10, run the Add Printer Wizard and select network printer instead of local printer. The following outlines the steps to install a network printer in Windows 10:

1. **Choose Start, type printer, and select the Printers & Scanners result.**
2. **In the Printers & Scanners settings panel, click Add a Printer or Scanner.**
3. **Select the network printer you want to print to.**  
Note that you will see network printers in this device listing only if your network administrator has given you permission.
4. **Click Add Device.**

The printer server that hosts the print device will deliver device drivers to your computer transparently.

In Windows 10, you have the nifty Print Management console to help you keep reign on your local and network printers. I show you the interface in [Figure 4-9](#); incidentally, this is the same tool Windows Server systems administrators use to manage enterprise-grade network print queues.



**FIGURE 4-9:** The Print Management console is a great Windows 10 tool that unifies and simplifies printer administration.

## *Printer sharing protocols*

Any shared printer nowadays makes use of the TCP/IP protocol suite and Ethernet networking. Some vendors, namely Apple, make use of special file and printer sharing protocols, like their Bonjour protocol.

WiFi-enabled printers operate at the various speeds that correspond to the IEEE 802.11 wireless protocol in use on the network:

- » **802.11a:** 54Mbps
- » **802.11b:** 11Mbps
- » **802.11g:** 54Mbps
- » **802.11n:** 600 Mbps
- » **802.11ac:** 1.3Gbps

Recall that WiFi networks can operate in one of two modes. In *infrastructure mode*, multiple clients (with network printers acting as one of those clients) attach to the WLAN through a wireless access point.

In *ad-hoc mode*, wireless peers connect directly to each other. Finally, for your A+ exam success, remember that some printers include integrated print servers that bundle a network interface, RAM, and disk cache. These devices are cool because they don't rely upon a separate computer to handle the print server duties.

## *Troubleshooting Printer Problems*

Printers are wonderful devices that we depend on day in and day out as we prepare, conduct, and report on our business. But one of the major downfalls of a world that depends on printers is that they never seem to work!

You discover a number of general troubleshooting guidelines in the sections that follow to help you troubleshoot printer problems. You also find out about a few specific problems with each type of printer.

### *Check the simple stuff first*

The first thing you want to do when you cannot print is to verify the simple stuff. The following is a list of simple things to check on the printer:

1. **Connection check:** The first thing you want to verify is that the printer is physically connected to the computer or network.
  - *USB:* If you have a USB printer, verify that the USB cable is connected to both the printer and the computer.
  - *Network:* If the printer has a network card, verify that the network cable connects the printer to the network properly and that you have network connectivity. After you verify that the network card is connected, you might want to check that the printer has an IP address by printing out the configuration of the printer. If you're using a wireless printer, you should recheck that the printer is in fact connected to the correct WLAN and that the printer uses the correct encryption protocol and key.

2. **Visual indicators:** After you checked the physical connection, look at the visual indicators on the printer to verify that it is powered-on. Make sure that you can see the online lamp that indicates that the printer is ready for use.
3. **Error codes:** While looking at the visual indicators on the printer, look at the printer for any error codes that help you identify what the issue is with the printer. Error codes are unique to each printer and are sometimes amber or red lights that turn on in different places to indicate the problem. You will need to research what those lights mean for your printer. Newer printers with an LCD will typically have text indicating what the error is, and some network printers can even be configured to email the error to the administrator!
4. **Out of paper:** After checking the error codes on the printer, you might as well take out the paper tray while you are at the printer and verify that paper is loaded. Usually, if you are out of paper, the printer will give an out of paper error, but it is worth the time to check.

## *Paper jams*

Another type of problem that occurs often is paper jams. If you experience a number of paper jams over and over again, verify that you are using the correct type of paper for the printer. The best thing to do here is to check the documentation of the printer and verify that you are using the correct size paper. If you are using paper that is too thick for your printer, it may jam a lot.

## *Garbled characters or corrupted output*

If you experience *garbled characters* (text that doesn't make sense) or corrupted output of any type, the driver is corrupt or you have the wrong driver installed. Printing a test page is one of the best ways to find out whether you have a bad driver or whether the application you are printing from is causing the problem.

To print a test page in Windows 10, follow these steps:

1. **Choose Start, type printer, and select the Printers & Scanners result.**



2. **Select your printer, and then click Manage.**
3. **In the Manage Your Device panel, click Print a Test Page.**

If you print a test page and the printout is still garbage text, the driver is likely corrupt, and you need to install a new driver by going to the properties of the printer and choosing the Advanced tab. On the Advanced tab, click the New Driver button to install a new driver.

### *Spots or smudging on the printout*

In general, spots or constant smudging on printouts are good indications that you are using the wrong type of paper for your printer. Again, check the documentation for the printer to find out what type of paper you should be using.

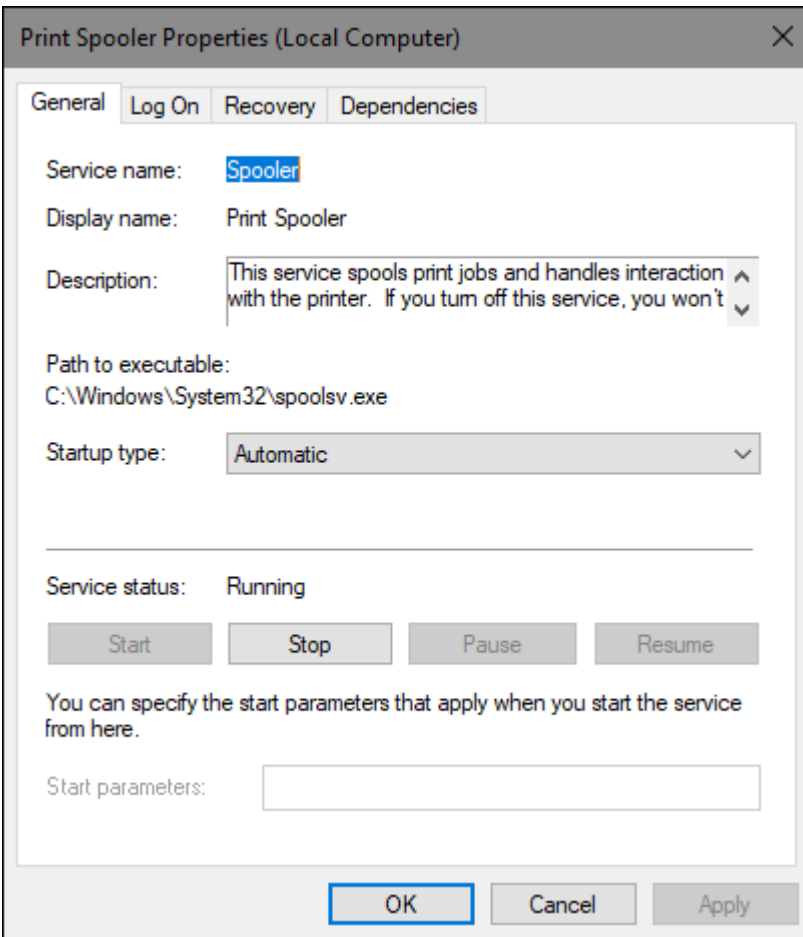
### *Slow printing*

If you notice that printing is overly slow, verify that spooling is enabled. Spooling is enabled by default, but it might have been switched to Print Directly to Printer when you were troubleshooting or configuring the printer. Check the properties of the printer and ensure that spooling is enabled.

### *Spooling service problems*

In Windows, the *print spooler service* is responsible for managing the printing environment. If you notice that a print job is hung in the print queue and will not print or you cannot delete it, you might have a corrupt queue.

When this happens, stop and restart the print spooler service in Windows. Stopping the print spooler service deletes all print jobs and essentially “reboots” your printing environment for you. [Figure 4-10](#) shows the print spooler service being restarted, which you can do from the Services console. The Service Control Manager console is found in by opening Start, typing **services.msc**, and pressing Enter.



**FIGURE 4-10:** Editing the spooler services properties on a Windows system.

If you have a number of problems printing in Windows and you determined that the problem is not hardware related, you might need to move the print spooler folder. By default, the print job is spooled to the hard drive at the `%systemroot%\system32\spool\printers` directory. The `%systemroot%` variable is typically the Windows folder on drive `C:`.

If you are running out of space on drive `C:`, you might want to change the partition for the spool directory. To change the default spool folder in Windows 10, follow these steps:

1. **Choose Start, type printer, and select the Printers & Scanners result.**
2. **In the Printers & Scanners settings pane, click Print Server Properties.**

The link can be difficult to find — look at the right side of the window.

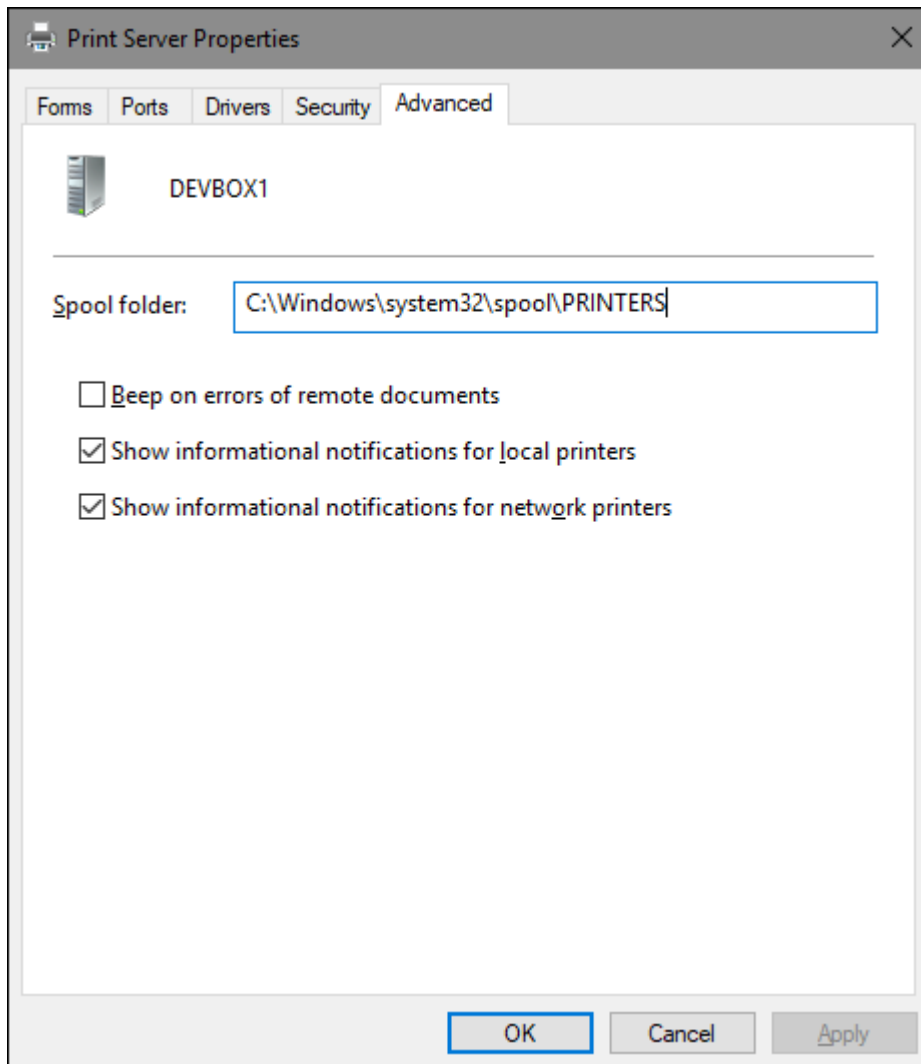
3. **In the Print Server Properties dialog, browse to the Advanced tab, as shown in [Figure 4-11](#).**

4. **Click Change Advanced Settings and authenticate as an administrator.**

You need to have elevated permissions to change the spool folder directory in Windows 10.

5. **Edit the spool folder directory path and click OK to complete the configuration.**

You should restart your computer to re-initialize the Spooler service.



**FIGURE 4-11:** Changing the spooling folder on a Windows 10 system.

## *Dot matrix problems*



**FOR THE  
EXAM**

This section identifies some problems that occur with dot matrix printers. Be sure to review these problems and the possible causes before taking the A+ exams:

- » **Faint printing:** If you experience faint printing with your dot matrix printer, the print ribbon is simply worn out and needs to be replaced.
- » **No printing:** If your dot matrix printer simply doesn't print, a print head cable might be disconnected, or the print head might have torn through the ribbon. In these cases, connect the print head cable or replace the ribbon.
- » **Paper jamming:** Again, a lot of paper jams is a great indication that you have the wrong type of paper or the wrong size paper. Check the documentation for your printer.
- » **Line across the page:** If your dot matrix printer prints a line all the way across the page, you might have a pin in the print head that is stuck out. You might be able to loosen the stuck pin, or you might need a new print head.

## *Inkjet problems*



**FOR THE  
EXAM**

This section identifies common problems that can occur with inkjet printers during day-to-day activity. Again, review these before taking your A+ exams:

- » **Paper jam:** A paper jam indicates that you might have the wrong type or size of paper. If you have the correct size paper, the feeder wheels

might be dirty — they are responsible for moving the paper through the printer.

- » **Poor print quality:** Having a poor-quality printout could indicate that the ink needs to be replaced or that you have the wrong type of paper. Change the ink or check the documentation to ensure you are using the correct type of paper.
- » **Fading/Ghosted print:** If the print from your inkjet printer is fading, that could be an indication that you need to change the ink.

## *Laser printer problems*

The following common problems can occur with a laser printer:

- » **Faint or ghosted print:** If the print is getting faint in your laser printouts, you most likely need to replace the toner.
- » **Paper jam:** If you get a lot of paper jams, verify that you are using paper of the correct size and thickness. If you are sure that you have the right paper, you could also have a problem with misaligned rollers.
- » **White stripes:** If you have white stripes throughout the printout, your transfer corona wire is most likely the problem. There might be a problem getting the charge to the paper, resulting in toner missing on the page in areas.
- » **Blank page:** If you have a blank page for output, you know there is nothing wrong with the feeder mechanisms because the paper is moving through the printer. A blank page indicates a problem getting the toner to the paper, so something is wrong with the corona wires or you have no toner.
- » **Vertical line:** A vertical line on the printout typically indicates a scratch in the print drum. You should replace the toner cartridge because it is combined with the print drum. If you replace the toner cartridge and the problem still exists, there could be a problem with the laser.

- » **Toner not fused to the paper:** If toner smears off after the page has printed, something is wrong with the fuser rollers, which might need replacing. Be cautious when working with the fusing components because they are very hot!
- » **Out of memory:** When sending a large document or a document with a lot of images to the printer, you might get an Out of Memory error if you do not have enough memory installed in the printer. The best solution is to add more memory to the printer so that it can handle the type of print jobs you send. Alternatively, send smaller print jobs to the printer or lower the print quality of the printout through the print settings.

## *Common problems and tools*

The following printer problems are common to many different types of printers:

- » **Streaks:** You may experience streaks on a printout with a laser printer due to the primary corona wire being dirty. To fix the problem, use a cleaning brush to clean the corona wire.
- » **Creased paper:** If you are experiencing creases in your paper when printing, it could be due to the registration rollers being worn out.
- » **Paper not feeding:** If you are experiencing any trouble with the paper not feeding through the system properly, you most likely are experiencing worn-out rollers.
- » **Backed-up print queue:** If you have a backed-up print queue, it is most likely due to a large number of print jobs being sent to the printer and the printer cannot handle the workload. Consider using a feature such as print pooling to speed your printing.
- » **Access denied:** If you experience an access denied error, have a look at the permissions on the printer.
- » **Printer will not print:** If the printer will not print, verify that a connection exists and then print a test page from the printer properties.

- » **Wrong color prints:** If you find that the printer is printing the wrong colors, you may be running low on ink of a particular color. Time for a refill!
- » **Unable to install printer:** If you are unable to install a printer, it could be because you do not have privileges to do so on the system. Log on as a system administrator and install the printer.

When troubleshooting problems, it helps if you have the right tools to do the job. The following are some common tools to help troubleshoot printers:

- » **Maintenance kit:** You can purchase a maintenance kit for your printer. This will give you all the tools you need to clean and maintain the printer. Note that maintenance kits are specific to a certain printer make and model.
- » **Toner vacuum:** A toner vacuum allows you to clean toner off other parts of the printer.
- » **Compressed air:** Compressed air is always great to have around to help dust off computer parts.
- » **Printer spooler:** The print spooler service is responsible for the printing in Windows. If you find that your print job is not printing and is stuck in the queue, restart the print spooler service to solve the problem.

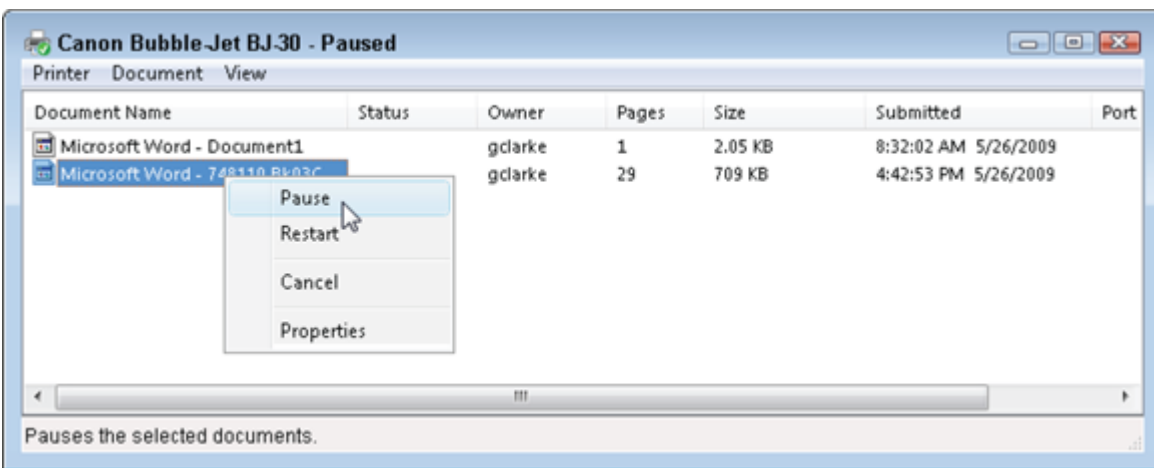
## *Managing print jobs*

When troubleshooting printing problems, it is important to be familiar with how to manage the print jobs. You can view the print jobs that are stuck in a printer (the print queue) by navigating to the Printers folder and then double-clicking the printer you are troubleshooting.

With the print queue open, you can perform a number of actions to manipulate the queue itself or a single print job. The following are the two major types of tasks that can be performed:

- » **Print jobs tasks:** Manipulate individual print jobs, such as pausing, resuming, or deleting a single print job.
- » **Print queue tasks:** Manipulate the entire queue. Just like a print job, you can pause, resume, and purge the entire queue.

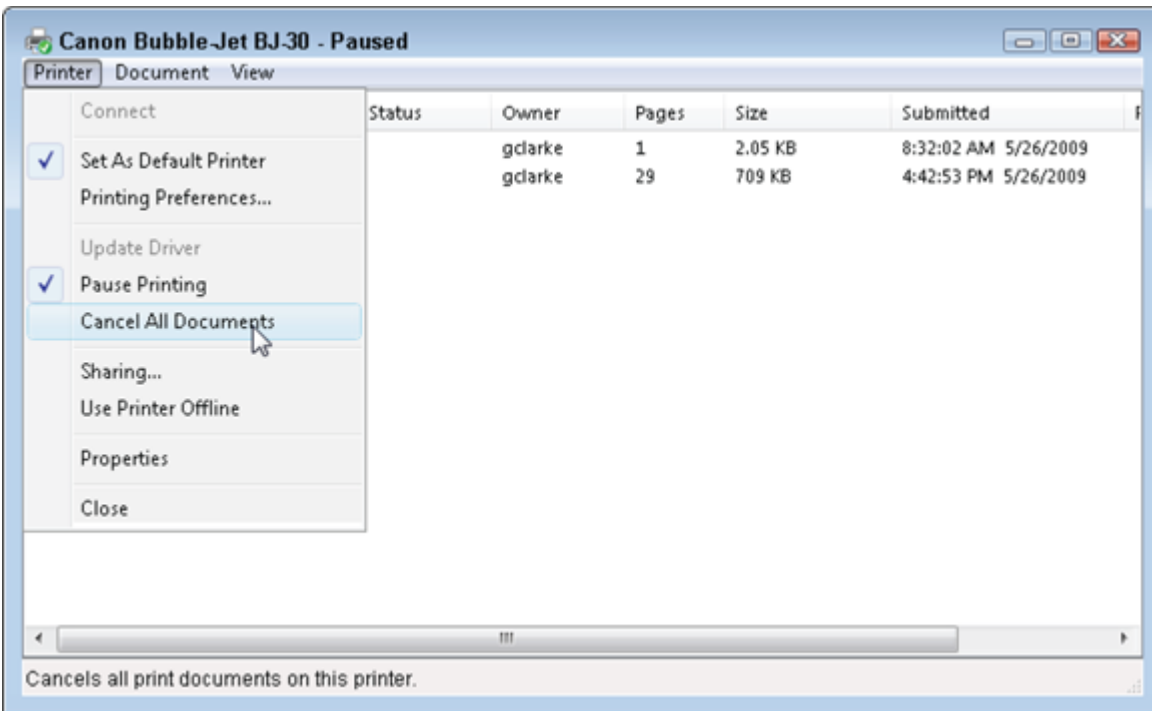
To manipulate a single print job, open the printer (double-click it) and view the list of current print jobs. To pause, resume, or delete a print job, right-click the print job and choose the appropriate command from the contextual menu (see [Figure 4-12](#)).



**FIGURE 4-12:** Managing a single print job within the print queue.

To manage the entire print queue, open the printer. Double-click the icon in the Printers folder. From the printer's folder, delete all print jobs, pause the queue, or resume the queue from the printer menu; see [Figure 4-13](#).





**FIGURE 4-13:** Managing the print queue.

The following are the popular menu options that deal with managing the print queue:

- » **Set as Default Printer:** Set the printer as the default printer. The benefit of flagging a printer as the default printer is when you click the Print button in an application, the document automatically prints to the default printer. Also, when you choose File ⇒ Print in an application, the printer is the printer selected by default to print to.
- » **Pause Printing:** Pause the entire print queue. To resume printing, choose Pause Printing a second time to toggle the option off.
- » **Cancel All Documents:** Delete all the print jobs sitting in the print queue.
- » **Properties:** View and change the printer settings that I discuss in the earlier “[Configuring a printer](#)” section of this chapter.

# *Understanding Safety and Preventive Maintenance*

In this section, I show you some common safety and preventive maintenance practices for printers.



**FOR THE  
EXAM**

For the A+ exams, be sure to review the safety points in Book 1, [Chapter 3](#), along with the safety and preventive maintenance points presented here.

## *Safety precautions*

The first point to make about working with printers is to be sure you turn off the printer and unplug it before doing any maintenance on it. Also be sure to give the printer time to cool down because there are many parts in the printer that can get very hot — especially with laser printers.



**WARNING**

If you are servicing a laser printer, be sure to give the printer time to cool down because the fuser rollers get very hot. These rollers are hot enough to melt toner to the paper, so they can cause severe burns to your skin. Be careful!

You also want to be cautious when working around toner because it can get very messy. Be sure not to get toner in your eyes or on your skin. If you have spilled toner, get a vendor-approved vacuum to suck it all up. If you have toner on your skin and want to wash it off, use cold water instead of hot water — you wouldn't want to fuse it to yourself!

## *Preventive maintenance*

*Preventive maintenance* for your printer will help reduce downtime.

Think of your relationship with your printer like any other relationship — if you treat the printer well, it will stick around; if you don't treat it well,

it'll leave you when you least expect it. Care for your printer by cleaning it every once in a while — at least once a year. (Make it an anniversary thing.)

To clean your laser printer, follow these general steps or consult the manufacturer's documentation for exact methods of cleaning your printer make and model. Some general steps to follow to clean the laser printer are:

1. **Turn off and unplug the printer.**
2. **Clean the outside of the printer with a lint-free cloth and a tiny bit of isopropyl alcohol.**
3. **Remove the paper tray and paper. Clean the tray, removing any dust or paper particles. Clean the area inside the printer where the tray resides.**



**REMEMBER** Be sure to clean the feeder rollers — they get pretty dirty.

4. **Open the printer and remove the toner.**
5. **Clean the inside of the printer; don't be afraid to clean the rollers.**
6. **Put the toner and the paper tray back in and print a test page.**



**ON THE  
WEB**

Lab 4-3 allows you the opportunity to review the steps to cleaning an ink cartridge on an inkjet printer. Lab 4-3 can be found on the companion website at [www.dummies.com/go/aplusaio](http://www.dummies.com/go/aplusaio).

Unfortunately, you end up troubleshooting printing issues on the network more than any other type of system issues, so be sure to read the previous sections on troubleshooting. You can help reduce problems with printers by performing the following regular maintenance on laser, thermal, or impact printers:

- » **Replacing toner/ribbon/impact paper:** You will need to replace the toner or ribbon on your printers from time to time as they run out or become worn out after so many print jobs. If you notice that the print quality changes over time, replace the toner or ribbon on the printer. You will also need to add paper to the printer, so be sure to find out where the paper loads.
- » **Replacing print head, ribbon, tractor feed:** These are the internal components that are most likely to fail with repeated use.
- » **Calibration:** *Calibrating* the printer is setting up the printer to print the color balance that you see on the screen. When you install new ink in a printer, you should first run the calibration feature on the printer to set up the correct distribution of colors to the paper.
- » **Cleaning:** You will need to remove debris on parts of the printer to ensure the quality of the printout. Always use the approved cleaning supplies for the printer to clean its parts.

## Getting an A+

In this chapter, you find out about three types of printers — dot matrix, inkjet, and laser printers. You discover how each printer prints and find out about the six phases of the laser printing process. The following are some key points to remember about printers when preparing for the A+ exams:

- » Laser printers use light, electromagnetism, and heat to create a printout.
- » Inkjet printers use a heating element to vaporize ink and spray it through a pinhole to make characters on a page.
- » Dot matrix printers use solenoids to strike a ribbon, creating characters from patterns of printed dots.
- » You may use a parallel connection, USB, or network connection to send the print job from the computer to the printer. USB is popular for

home and small office use, and larger companies typically use a printer with a built-in network card.

- » The six phases to the laser printing process are charging (conditioning), writing, developing, transferring, fusing, and cleaning.
- » You may install a printer in Windows via the Add Printer Wizard. After the printer is installed, you can configure a number of settings, such as spooling, scheduling, and priority.

## *Prep Test*

### **1. What are the two types of feeder mechanisms used in printers?**

- (A) Continuous tractor feed
- (B) Continuous form feed
- (C) Friction feed
- (D) Injected

### **2. Which of the following devices use friction feeder mechanisms? (Choose two.)**

- (A) Laser printers
- (B) Fax machines
- (C) Dot matrix printers
- (D) A printer that prints hundreds of payroll checks

### **3. A positive charge is applied to the paper by which laser printer component?**

- (A) The laser
- (B) The print drum
- (C) The registration rollers
- (D) The transfer corona wire

**4. What is the purpose of the negative charge on the print drum of a laser printer?**

- (A) To attract the toner to every area of the drum
- (B) To attract the toner to the areas of the drum that have a stronger negative charge
- (C) To attract the toner to the areas of the drum that have a weaker negative charge
- (D) To attract the positively charged paper to the print drum

**5. Why are both the developer roller and the print drum charged with  $-600\text{V}$  in a laser printer?**

- (A) So the paper is attracted to neither
- (B) So the toner is attracted to neither
- (C) So the toner creates a fusion cloud between the two rollers and the paper
- (D) So the toner is attracted only to weakly charged areas of the print drum

**6. The paper is charged with which voltage charge by the secondary corona wire?**

- (A)  $+600\text{V}$
- (B)  $-600\text{V}$
- (C)  $-100\text{V}$
- (D)  $+100\text{V}$

**7. What method does an inkjet printer use to print a page?**

- (A) One dot at a time to form a character
- (B) Spray-painting a character
- (C) Striking an inked ribbon
- (D) Dropping ink onto the paper

- 8. With an inkjet printer, what causes the ink to vaporize?**
- (A) Electrical charge
  - (B) A heating element within the ink cartridge
  - (C) A solenoid in each chamber of the ink cartridge
  - (D) Drying of the ink when the cartridge has not been used for some time
- 9. A vertical line on every page of a printout from a laser printer indicates what?**
- (A) Fleck of toner
  - (B) Scratch on the print drum
  - (C) Light leakage
  - (D) Fingerprint
- 10. What would you do if the print job refused to leave the print queue in Windows 10?**
- (A) Delete the printer and re-install it.
  - (B) Restart the computer.
  - (C) Turn the printer off and then on.
  - (D) Stop and restart the spooler service.

## *Answers*

1. **B, C.** Continuous form feed and friction feed are the two types of paper feeder mechanisms. Dot matrix printers use continuous form feed, and laser printers use friction feed. See “[\*Learning about Paper Feeder Mechanisms\*](#). ”
2. **A, B.** Friction feeders use rollers that apply pressure and friction to the top sheet of paper in the paper tray to move it into the print device. Laser printers and fax machines use friction feed. Review “[\*Friction feeders\*](#). ”

3. **D.** The transfer corona, also known as the secondary corona wire, charges the paper with a +600V charge. Check out “[The laser printing process](#). ”
4. **C.** The print drum is charged with an initial –600V charge. The laser writes the image onto the print drum by weakening the charge to –100V in areas that create the image. This causes the toner to attract to the –100V areas because the toner is approximately –600V — and opposites attract! Peruse “[The laser printing process](#). ”
5. **D.** The developer roller and the print drum are equally charged so that they are repelled from one another. The toner on the developer roller will be attracted to neutralized areas of the print drum caused by the laser. Take a look at “[The laser printing process](#). ”
6. **A.** The transfer corona charges the paper to +600V, so the toner on the print drum is strongly attracted to it. Peek at “[The laser printing process](#). ”
7. **B.** An inkjet printer sprays the ink onto the paper. Look over “[Inkjet printers](#). ”
8. **B.** Within the ink cartridge, a heating element vaporizes the ink, forcing it to spray a drop out the pinhole in the nozzle. Study “[Inkjet printers](#). ”
9. **B.** A scratch on the print drum can cause a vertical line to appear in the printout. Refer to “[Laser printer problems](#). ”
10. **D.** You would stop and start the print spooler service, deleting everything from the queue. Stopping and starting the service is a way of rebooting the printing environment. Examine “[Spooling service problems](#). ”



# Chapter 5

## Working with Multimedia Devices

---

### IN THIS CHAPTER

- » Understanding scanners
  - » Understanding digital cameras
  - » Working with other multimedia devices
- 

It is amazing to see an old uncle at a birthday party who just a few years back had not even touched a computer but now snaps photos with his digital camera and drones on about how simple it is to upload the pictures to his computer and then burn them to a DVD! When I try to think of examples of how computers have entered our daily lives, this is the most promising example I can think of.

In this chapter, you find out about popular multimedia devices used in everyday life. In the following pages, I discuss a number of multimedia devices, starting with digital cameras and scanners — the two most popular types of computer-related multimedia devices. I also introduce a few key points about microphones and MIDI technology, which are very important to the many people who will record music through their computers and are objectives covered by the A+ certification exams.

## *Understanding Scanners*

In this section, you find out about different types of scanners. I also show you how to scan a photo in Windows 10 and how to save the photo as a file on the computer.

A few years back, scanners were very popular because they were one of the only ways to get your photos into a digital format. Maybe you wanted to use the computer to alter the photo or to send it to a relative via email. To do any of these actions, you had to use a scanner, which would copy the photo as a digital image that could be saved on your computer.

Many different types of scanners have been manufactured over the years, and you need to be familiar with the different types of scanners for the A+ certification exams. They are

- » **Flatbed:** The flatbed scanner is the most popular scanner today. With a flatbed scanner, you lift the cover of the scanner and place the photo on the flat sheet of glass (a *platen*). A scan head then moves beneath the picture, scanning the image by using a piece of technology called a *charge-coupled device* (CCD). [Figure 5-1](#) shows a flatbed scanner. Nowadays you'll often find flatbed scanners integrated into a multi-function device (MFD). MFDs combine print, fax, and scan into a single unit.
- » **Handheld:** A handheld scanner is great where it is impossible to place the object to be scanned on a flatbed scanner. To use a handheld scanner, you move the scanner over the object that you want to scan.
- » **Sheetfeed:** A sheetfeed scanner acts very much like a fax machine in the sense that the scan head is stationary. You insert the paper object to be scanned, and the feeder passes the paper over the scan head. This scanner type looks very similar to a portable printer and is also the scanner type typically found in multifunctional printers.
- » **Drum:** A drum scanner uses a technology called a *photomultiplier tube* (PMT), which involves wrapping the photo around a glass tube. The drum releases light that is converted to electrical data to become the image file.



**FIGURE 5-1:** A flatbed scanner uses a scan head that moves under the object being scanned.



**FOR THE  
EXAM**

You need to be familiar with the different types of scanners for the A+ exams.

## ***Scanning process***

Most scanners use a CCD, which is responsible for capturing the photons created by the light being exposed to the picture and then converting those photons to electrons, which are a form of electrical data. The image is then created from the electrical data.

The scanner has a scan head that contains the CCD along with a number of mirrors and lenses. The mirrors reflect the light from the lamp onto the photo being scanned. That light then passes through the lenses to the CCD to create the image.

## *Connecting a scanner*

You can use a number of different types of ports to connect a scanner to the computer, depending on what type of connection your scanner wants to use. The popular ports used by a scanner are as follows:

- » **SCSI:** Another popular form of scanner connection a few years back was the SCSI (Small Computer System Interface) connection. To connect a SCSI scanner to a computer, make sure that you
  - Have an SCSI host adapter.
  - Assign a unique ID to the scanner.
  - Terminate the SCSI bus.
- » **USB:** The most popular method used to connect a scanner to a computer these days is the USB (Universal Serial Bus). With USB, you simply connect the scanner to the computer, and Plug and Play kicks in and either loads the driver or prompts you for it.

## *Scanning an image*

In this section, I show you how to scan an image in Windows 10. You will most likely not be tested on the actual scanning of a document or picture for the A+ exams, but you may need to scan a document on the job. For this discussion, I assume that you already connected the scanner and loaded the driver for the device.

Although the procedure here assumes you're using the Windows-provided Plug and Play driver, you should always install the software included with your printer. This vendor-specific software almost always gives you more flexibility and more features than the PnP driver does.

Keep in mind you'll likely get better options and performance if you use your scanner manufacturer's scanning software. Nevertheless, follow these steps to scan a picture in Windows 10 using native tools:

1. **Choose Start, type scan, and select the Scan a Document or Picture search result.**

If your scanner is plugged in and turned on, the scan app lists your scanner's name and the file type used for saving your files. (The PNG file type is widely accepted by most programs.)

**2. To change settings, click the Show More link.**

The app's default settings work fine for most jobs.

**3. Click the Preview button to make sure your scan appears correct.**

**4. Click the Scan button.**

**5. When the scan finishes, click the View button to see your scan.**

The Scan app scans your image with the settings you've chosen in the previous steps and then saves your image in your Pictures folder's Scan folder.



**TIP** The scanned images are stored in the Pictures folder in Windows 10 by default.

## *Using Digital and Web Cameras*

Several years ago, back in the days when I walked uphill to and from school in the driving rain, taking pictures involved buying film for your camera, snapping some pictures, and then taking the exposed film to a photo lab to be developed — often only to find out that of the 24 pictures you took, only 4 of them were any good!

Photography has changed dramatically since then. Today, you can use a digital camera, which stores the picture in memory on the camera, not on film. You can also navigate through the pictures by using the built-in viewer on the camera and then delete the ones you do not like — then print only the ones you want developed!

The following sections introduce you to digital cameras, digital video cameras, and web cameras (webcams).

### *Digital cameras*

A digital camera is different from a conventional camera because instead of storing the image on film, a digital camera stores the image as a digital file on the camera. This file can then be uploaded to a computer and can be used in any application on the computer, such as email, presentation software, or a photo editor.

The digital camera works the same way that a scanner does — it captures light and uses a CCD to convert the captured light into an electrical charge that is used to create the pixels in the image. The light is captured through the lenses on the digital camera and is then passed through the CCD so the CCD can do its job of converting the light into data.



**TIP**

When shopping for a digital camera, you want to be sure you get the best camera for your dollar. The quality of a digital camera is measured in its resolution and zoom levels.

### ***Camera resolution***

Camera resolution is measured in pixels, just like monitor resolution. The more pixels recorded in the photos being taken, the more detail displayed in the picture. The resolution also affects how large the picture can become before becoming grainy. A camera advertises its resolution by indicating how many pixels it supports, which is typically measured in *megapixels* (MP; or millions of pixels). The higher the number of pixels supported, the better quality image you will get from your camera. Here are what some common camera resolutions translate into:

- » **4MP:** Supports an image resolution of 2240 x 1680
- » **5MP:** Supports an image resolution of 2560 x 1920
- » **6MP:** Supports an image resolution of 2816 x 2112
- » **8MP:** Supports an image resolution of 3264 x 2448
- » **11MP:** Supports an image resolution of 4064 x 2704
- » **12MP:** Supports an image resolution of 4368 x 2912
- » **14MP:** Supports an image resolution of 4416 x 3312

» **16MP:** Supports an image resolution of 4608 x 3456

By way of comparison, a 50MP camera is professional quality. At the time of this writing, the typical consumer-grade digital camera has a resolution of around 24MP.

Most digital cameras allow you to specify which resolution you would like to take photos in. For example, on my 16MP camera, I can specify that I want to take pictures with a resolution of 4MP, which creates a smaller image file but also creates a lower-resolution image. But if I am happy with the quality of my 4MP images (they are fine for eBay!) because they are smaller files, I can store more of them on the camera.

## *Zoom*

Digital cameras can have two types of zoom, optical and digital, both of which let you zoom in on your subject when taking a photo. In the following list, optical and digital are compared against what is known as *fixed focus*:

- » **Fixed focus:** A *fixed focus camera* does not support any type of zooming features. What the camera sees is what the camera takes as a picture. To zoom in, you need to physically get closer to the object. This is the zoom type (actually a lack of zoom) used on disposable cameras.
- » **Optical zoom:** *Optical zoom* is the “good” zoom type that uses lenses on the camera to change the focus and zoom in on the object. This zoom type does not alter the image in any way: It simply zooms in and takes the picture.
- » **Digital zoom:** Digital zoom is what I like to refer to as a *virtual zoom*. It takes the picture and then goes to the center of the image and magnifies the subject. This is the same as you taking an original photo into a photo editor and magnifying the image and then cutting to the part you like. This typically never turns out right because as you magnify the image, it becomes grainy.

## *Uploading pictures to the computer*

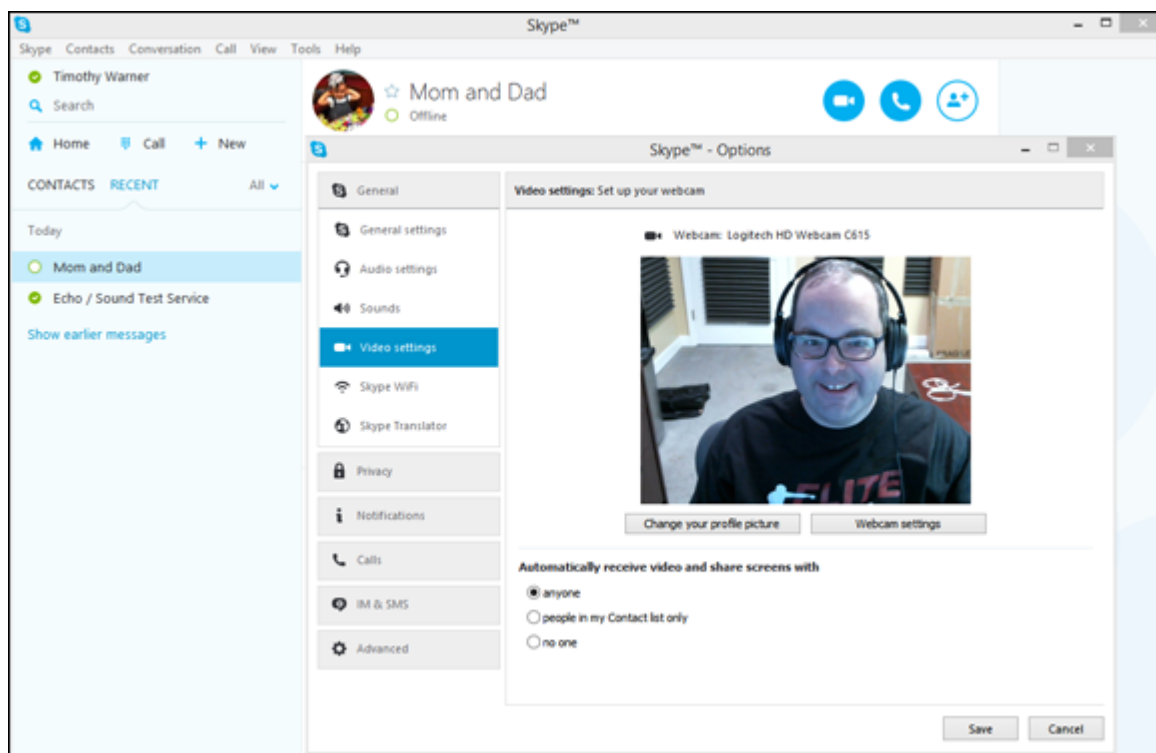
The steps to upload pictures from your digital camera in Windows 10 are pretty easy — you simply plug the camera into the computer and power it on, and the Autoplay window in Windows 10 will appear asking how to upload the pictures. If you choose Import Pictures, the Import Pictures Wizard will launch asking you to tag a name to this group of pictures. It then copies the pictures to the system.

## *Web and digital video cameras*

In this section, I introduce you to web cameras, digital video cameras, and the concept of a codec, all of which are important to understand when supporting video devices or video applications.

### *Web cameras*

*Web cameras* (also called *webcams*) can capture video and display it on the computer screen, or they can be used to record a video and store it in a digital format on the computer. Webcams are popular with conferencing applications, which allow you to have a live conversation while seeing the person you are talking to, over the Internet. An example of an application that can use a webcam is Skype (see [Figure 5-2](#)).





**FIGURE 5-2:** Webcam-enabled applications like Skype let you chat or video conference.

A webcam is typically shaped like an eyeball with a lens on the front and connects to the system's USB port. Most webcams have a stand that holds the camera and allows it to sit on the monitor or desk. There are also laptop versions of webcams that clip to the frame around the laptop's LCD and also a number of laptops today have a webcam built-in to the LCD. [Figure 5-3](#) shows a webcam.



**FIGURE 5-3:** A webcam captures live video and sends it to anyone you are conferencing with.

### ***Digital video cameras***

Just like digital cameras have replaced conventional methods of taking snapshots, recording video with a digital video camera has become popular in this day and age. A digital video camera can record directly to

the computer and store the video as a file on the computer, or it can store the video to memory on the camera. It can also store the information to a digital video tape that can then be played later and recorded on the computer as a file.

A digital video camera typically connects to the computer via a USB 2.0 or 3.0 interface.

### *Understanding codecs*

The problem with digital video is that with all the information that needs to be recorded, the files can quickly become huge. Digital video file sizes are kept to a minimum by compressing the video using special *compression/decompression* (codec) software. There are a number of different types of video formats and codecs; some of the old standards include:

- » **DV:** Digital video cameras have their own proprietary format to store the video, known as the DV format. The DV format typically has no loss in quality.
- » **DivX:** DivX is one of the most popular codec types today. It supports high-quality video with high compression ratios. A video using the DivX codec uses only about 15 percent of the disk space that other codec types do.
- » **MJPEG:** MJPEG is based on the JPEG compression standard used to compress still images. This compression type is optimized for transferring video to and from tape but is not suited for Internet applications because special hardware is required to play the video back.
- » **MPEG1:** MPEG1, developed by the Moving Picture Experts Group, has been used heavily for creating videos to be distributed over the Internet because of its small file sizes and because only the codec is needed to play the video back.
- » **MPEG2 and MPEG4:** The MPEG1 video compression has been improved again and again to create the MPEG2 and MPEG4 compression standards, which have better compression rates and

better resolution. For example, the MPEG2 standard offers four times the resolution of MPEG1.



**REMEMBER** The important point to remember with codecs is that you must have the same codec installed on your computer that was used to record the video in the first place. Otherwise, the computer will not know how to decompress the video. If you do not have the correct codec, you will not be able to play the video.

## *Looking at Other Multimedia Devices*

Two other multimedia devices that are popular in today's systems are MIDI devices and microphones. Sound cards typically have a microphone port (also known as a *mic port*) and a MIDI port.

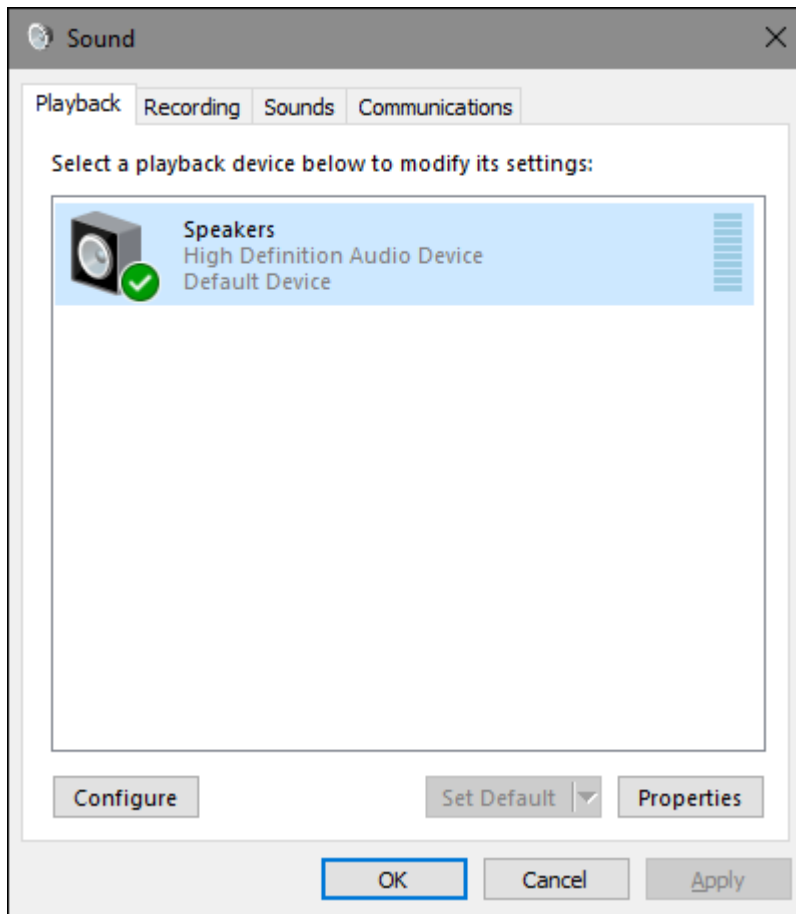
### *Microphones*

The microphone port on the computer is indicated with a little pictograph of a microphone. You can use the microphone port to plug a standard microphone into the computer. If you have a microphone whose cable will not connect in the mic port, you need to head to your local electronics store and find an adapter. After you plug in the microphone, you can use it as a recording source as long as you have specified it as a recording source in Windows.

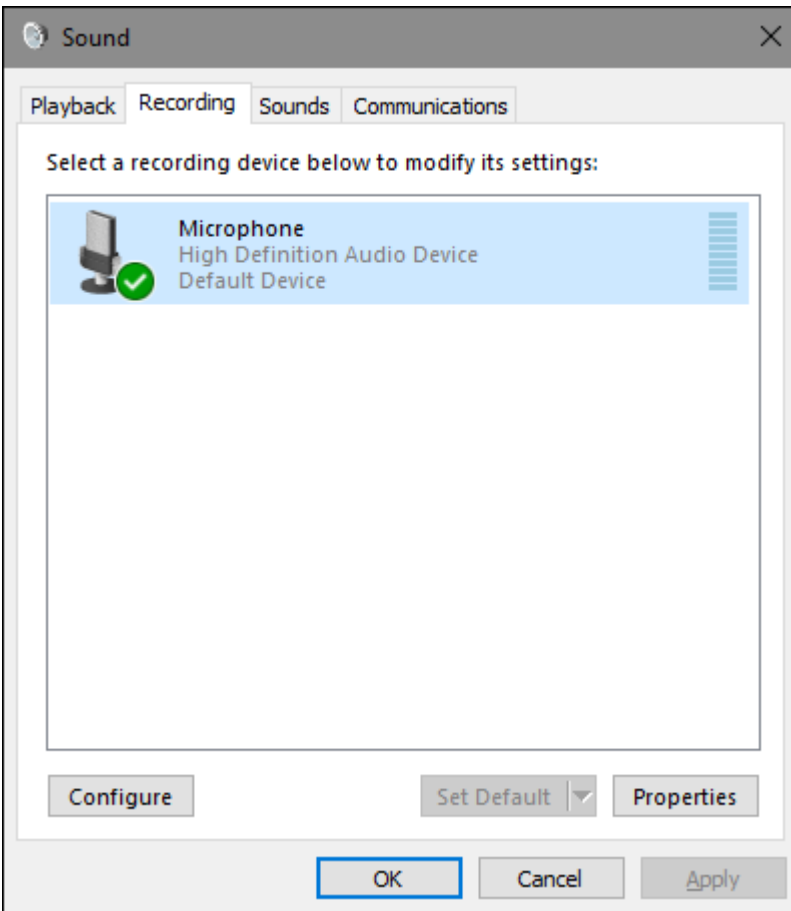
To set the microphone as a recording source in Windows 10, follow these instructions:

1. **Choose Start, type sound, and click the Sound control panel result (see [Figure 5-4](#)).**
2. **In the Sound control panel, navigate to the Recording tab, as shown in [Figure 5-5](#).**

3. Ensure your desired microphone is selected, and if it isn't, right-click it and select **Set as Default Device**.



**FIGURE 5-4:** Managing recording and playback devices in Windows 10.



**FIGURE 5-5:** Ensure the microphone is set as a recordable device.

## ***MIDI***

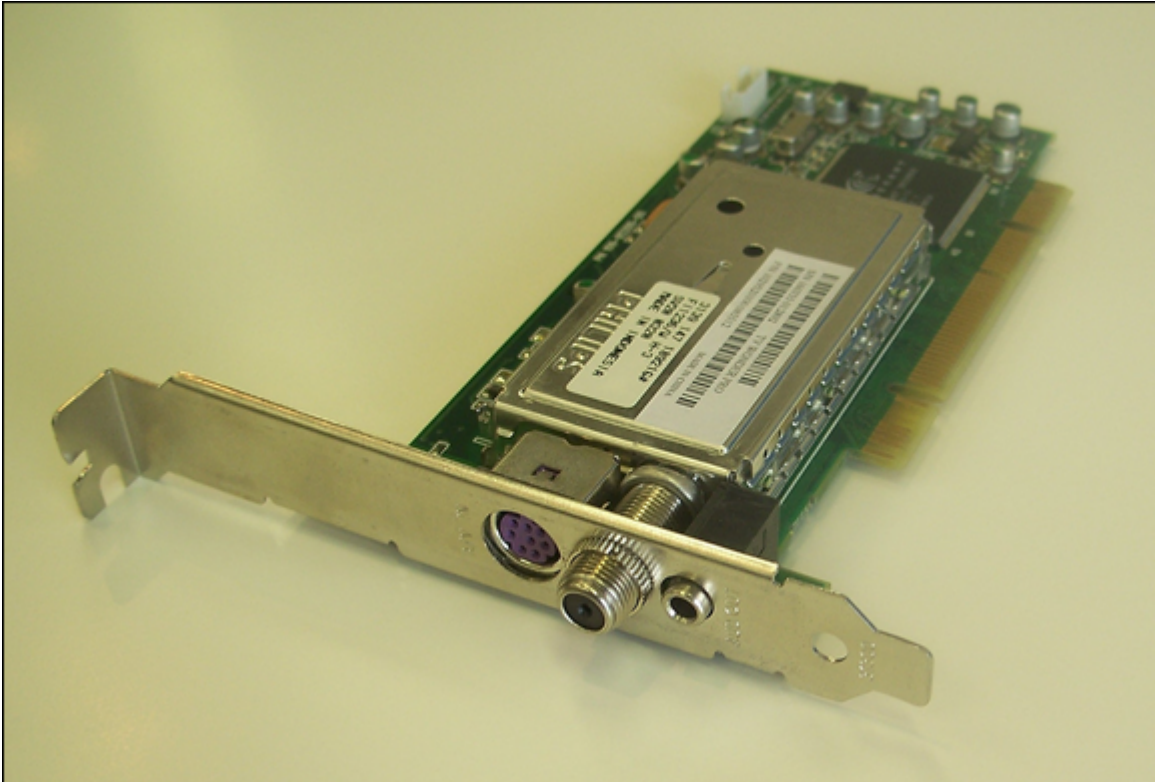
*Musical Instrument Digital Interface (MIDI)* is a standard developed to allow musical instruments to communicate with one another or with a computer. MIDI is a common language that all MIDI-capable instruments can speak. To use MIDI, you must have a MIDI-capable instrument — for example, a keyboard with a MIDI port on it — and a system with a MIDI port. You do not need to worry about the details of MIDI for the A+ exams.

## ***TV tuners, video capture cards, and camcorders***

The days of having to sit in front of a big television to watch your favorite TV shows are over. If you are interested in watching TV on your computer, just add a TV tuner card to your system. The TV tuner card has

a connector with which you connect the TV cable to the computer to receive the television signal so you can watch TV on the computer.

Most TV tuner cards act as video capture cards and come with software that allows you to record TV shows to video files on the computer that can be played back at a later time. [Figure 5-6](#) shows a TV tuner card. Most TV tuner cards come as PCI, PCIe, or USB devices.



**FIGURE 5-6:** Use a TV tuner card to receive a TV signal on a computer.

A camcorder can be connected to the Windows system to either use the camcorder as a video source for video capturing or to upload videos recorded on the camcorder. You typically connect the camcorder to the computer using either USB or FireWire. After the camcorder is connected to the system and the power is turned on, you should have the Windows Import Wizard appear, asking if you want to import the videos like you would pictures.

## *Virtual reality (VR) headsets*

A VR headset is a heads-up display (HUD) that enables you to participate in immersive applications. Many popular VR apps are games, but VR is being used increasingly to in the business world. For instance, a construction company can model a building it is designing and allow architects to “walk through” the structure virtually in a simulated three-dimensional environment.

Most VR headsets require a powerful computer to serve as its back end. However, the simplest VR applications enable you to insert your smartphone horizontally into a frame and display the simulation through that rudimentary headset.

### *QR scanners*

Quick response (QR) codes are rectangular images that encode a website uniform resource locator (URL). You can use a QR scanner app on your smartphone to focus on a QR image; the reader software translates the image to a URL, your browser opens, and you’re at the target site.

Many businesses include QR images in their advertising to make it easier for prospective or current customers to visit their websites.

### *Signature pads*

Signature capture pads are multimedia devices that are ubiquitous in stores with their point-of-sale systems. As you know, credit card purchases often require a signature. You use a stylus to “draw” your analog signature on the capacitive pad, and the reader transmits a digital representation of your signature to the e-commerce system and attaches it to your purchase.

Other use cases for signature pads are adding a signature to an ID card, signing forms, or signing receipts.

## *Getting an A+*

This chapter introduces you to some of the different devices used when working with multimedia and multimedia applications. Here are some key points to remember about multimedia devices:



- » A flatbed scanner is the popular type of scanner and uses a technology called a charge-coupled device (CCD). The scan head on the scanner moves under the image, exposing the image to light that is captured and then converted into electrical data by the CCD, which creates the image.
- » The most popular connection used by scanners and digital cameras is USB 2.0 or USB 3.0.
- » Digital cameras are measured by the quality of image they provide. The measurement unit is megapixels — millions of pixels. The larger the number of megapixels, the higher the resolution and the larger the image.
- » Codecs compress videos so that they do not use up as much hard drive space. To play a video on the computer, you need the same codec installed on your system that was used to compress the video.
- » If you are having trouble with your microphone picking up the sound around you, make sure that the microphone is set as a recording device.

## *Prep Test*

- 1. What type of scanner is portable and is swiped over the object to be scanned?**
  - (A) Flatbed
  - (B) Handheld
  - (C) Sheetfeed
  - (D) Drum
- 2. What technology do flatbed scanners and digital cameras use to create an image?**
  - (A) OCC
  - (B) CCO
  - (C) PMT



(D) CCD

**3. What zoom type on a digital camera simply magnifies the image to emulate the zooming feature?**

- (A) Fixed zoom
- (B) Digital zoom
- (C) Optical zoom
- (D) Pixel zoom

**4. Modern digital video cameras typically use which type of connection to connect to the computer and upload the video?**

- (A) SCSI
- (B) Bluetooth
- (C) FireWire
- (D) USB 2.0

## *Answers*

1. **B.** A handheld scanner is carried around by the user, and the scanner is moved over the object to scan the object. See “[Understanding Scanners](#).”
2. **D.** *Charge-coupled device* (CCD) is the technology used by flatbed scanners and digital cameras to create the image. Review “[Understanding Scanners](#).”
3. **B.** Digital zooming is the zoom type that simply magnifies the image, just like you would do yourself in image editing software. This could make the image appear grainy. Check out “[Digital cameras](#).”
4. **D.** While it was true that older digital video cameras typically used IEEE 1394 (FireWire) connections to connect to the computer, modern-day camcorders almost exclusively employ USB 2.0 or 3.0. Peruse “[Digital video cameras](#).”

## Chapter 6

# Dealing with Laptops and Mobile Devices

---

### IN THIS CHAPTER

- » Identifying portable computer components
  - » Looking at laptop batteries
  - » Understanding AC adapters
  - » Finding out about LCD panels
  - » Upgrading and expanding a laptop
  - » Mobile device operating systems
  - » Troubleshooting laptop issues
  - » Examining handheld mobile devices
  - » Securing mobile devices
- 

In this chapter, you find out about portable computers and their supporting technologies. On the A+ exams, you're required to identify characteristics of a laptop, such as the types of batteries and displays, and also how to upgrade a laptop's hard drive or memory.

Laptops gained popularity years ago because of their small size and mobility. I suppose you could carry around a standard desktop computer, but that is pretty inconvenient and causes wear and tear on your biceps. And even if you are willing to lug around a big, heavy desktop computer, the other problem with desktop computers is that you will not always have a power outlet to plug it into. A big benefit of laptops is that they use a battery as a power source, which is great when you're on a plane or out on safari and don't have a wall outlet.

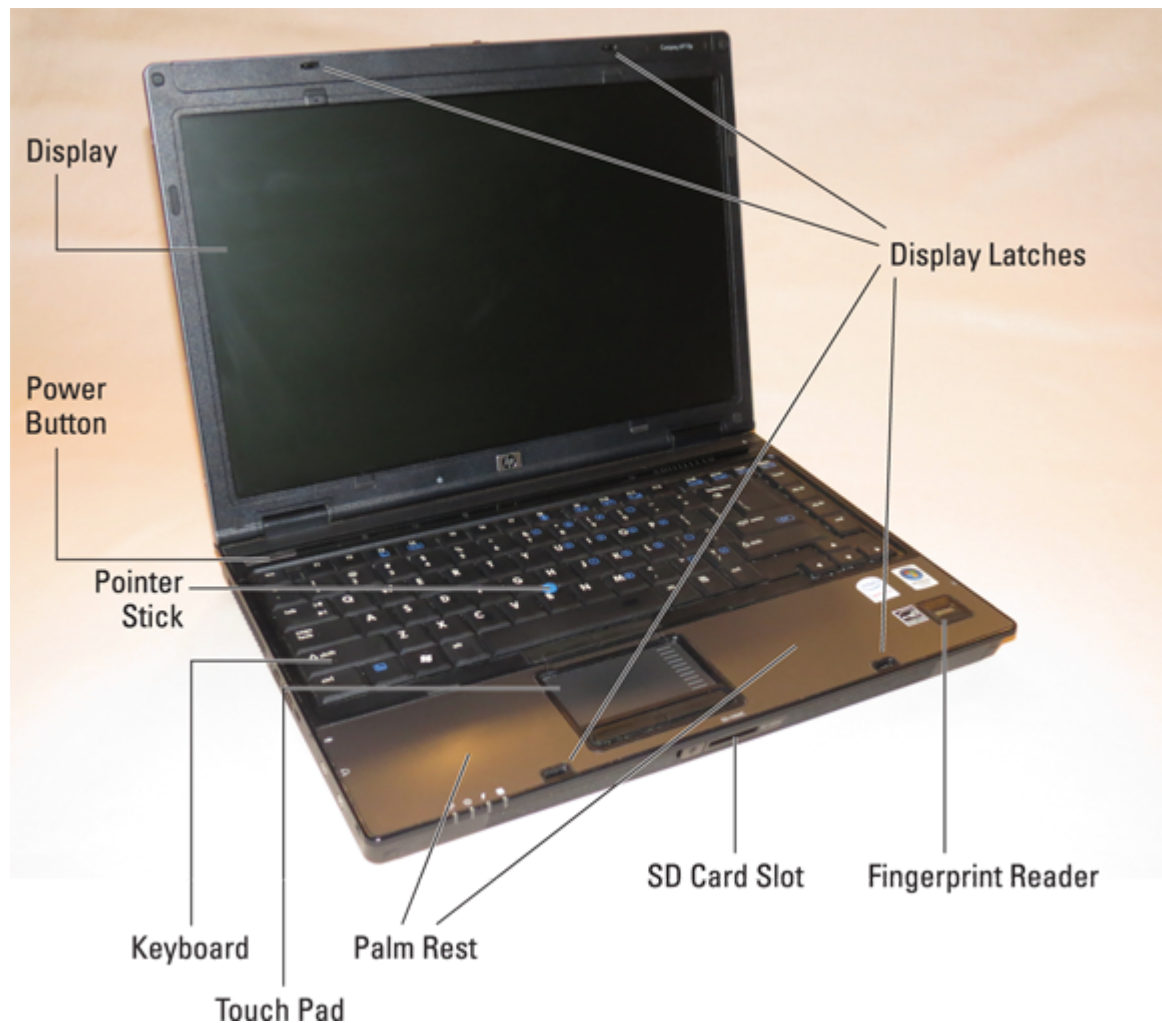
Although laptops are the portable computer type to focus on for the A+ certification exams, you should also be familiar with smartphones, which are ubiquitous practically worldwide by now.

In the current computing environment, these PDAs now take the form of smartphones, tablet computers, and smart watches (so-called “wearables”). Smartphones combine cellular phone technology with tablet computing functionality in a mobile phone-size package.

This chapter helps you identify, install, configure, and upgrade special portable computer components, such as batteries, hard drives, and memory. Procedures in this chapter guide you through the installation and removal of these components on laptop computers.

## *Identifying Portable Computer Components*

Although a number of different laptop brands are on the market, each make and model of laptop has common components. This section introduces you to some of the common components found in laptop computers. [Figure 6-1](#) displays these components.



**FIGURE 6-1:** Identifying the major components of a portable computer.

The following is a quick description of some of the major components found on laptop computers. Some of these components are also found on desktop computers and serve the same purpose for the laptop. For example, a video board built into a laptop does the same thing as a video board built into a desktop computer.

- » **Battery:** The *battery* supplies power to the laptop and its components. The battery is charged or maintains its charge from an AC adapter that plugs the laptop into the wall outlet.
- » **AC adapters:** The *AC adapter* supplies power to the battery so that the battery can either recharge or pass that power on to the laptop components.

- » **DC controllers:** The *DC controller* is responsible for protecting devices such as cards, chips, adapters, and circuitry from power surges. All internal components of the laptop, with few exceptions, are powered by DC power.
- » **ExpressCards:** This interface replaces the ancient PC (PCMCIA) standard. Nowadays you can buy just about any kind of expansion as an ExpressCard: modems, network cards, cellular service cards, audio cards, and so on. A cellular service card may be sold in ExpressCard format, although USB is just as popular nowadays.
- » **Video adapters:** The *video board* is responsible for converting the digital data from the system into information that the display can use to create the image. Video adapters are also sometimes informally called video cards.
- » **LCD panels:** The primary display type on laptop computers is liquid crystal display (LCD). LCD panel monitors are increasingly replacing CRT (cathode ray tube) monitors for desktop computers as well.
- » **Keyboard:** The keyboard found on laptops works the same way as a keyboard for a desktop computer. However, laptop keyboards are smaller versions of desktop computer keyboards, and some keys (such as the navigation keys) are in different locations than a traditional desktop keyboard.
- » **Hard drives:** Laptops ship with hard drives that are physically much smaller than those in desktop computers, typically use less power, and store less information.
- » **Memory:** RAM is installed in laptop computers in a similar fashion to desktop computers. The only difference is the type of memory modules, known as *small outline dual inline memory modules* (SODIMMs), used on laptop computers today.

Because laptops pack a lot of power into a very small space, that makes them susceptible to theft. To counteract this risk, laptops come with a small slot that can be fitted with a locking mechanism. These locks may be in the form of braided cable, similar to a bicycle lock, or may be a high-tech alarm. These options are discussed in Book 4, [Chapter 1](#).

# *Looking at Laptop Batteries*

Laptop computers ship with a battery that can be removed or replaced at any time. The battery acts as the primary source of power for the laptop and all its components. The battery maintains its charge, or is recharged, by an AC adapter that plugs the laptop into the wall. The AC adapter converts building AC into DC for the laptop and connects to the laptop through a DC jack. The following sections outline everything you need to know about portable-computer batteries for the A+ exams.

## *Different types of batteries*

It is important to understand that a laptop computer has two types of batteries: a main battery and a CMOS battery.

- » **Main battery:** This battery supplies power to the laptop and its components. A laptop is designed to work with one of four types of main batteries:
  - *Alkaline:* Typically found in palmtop computers; the same battery type you find in calculators.
  - *Li-Ion (lithium-ion):* Has a lot more battery charge time than a NiCad battery. A Li-Ion battery is also more expensive than a NiCad battery.
  - *NiMH (nickel-metal hydride):* Environmentally friendly because they do not contain toxic materials. They are the same weight as NiCad batteries but are more expensive and don't last as long as a Li-Ion battery.
- » **CMOS battery:** Just like a desktop computer, a laptop computer has a CMOS battery that is responsible for holding a charge to CMOS RAM so the CMOS configuration can be maintained. You can see a CMOS battery later in this chapter in [Figure 6-7](#).



FOR THE  
EXAM

On the A+ exams, if you are asked which battery is the best battery for laptop computers, the answer is a Li-Ion battery because it provides the most durability and performance. It is more expensive than the other types of batteries, though.

Another type of battery that you might hear of from time to time is a smart battery. A *smart battery* has its own power circuitry, which is responsible for monitoring the battery performance, output voltage, and temperature and also communicates the status of the battery back to the system. A smart battery is 15 percent more efficient than the other battery types and is also the most expensive type.

## *Handling batteries*



**WARNING** Before you handle any batteries, be forewarned that batteries contain toxic chemicals that can cause harm if the battery explodes. Be sure to follow these guidelines when handling batteries:

- » **Keep batteries away from fire and water.**
- » **Never open or dismantle a battery.**
- » **Try not to drop and never throw a battery.**
- » **Be sure to follow the manufacturer's guidelines when working with the battery.**

For example, if you're storing the battery, check the documentation on suitable areas for storage.

## *Maximizing battery performance*

One of my major pet peeves with batteries is that over time, the charge time of the battery fades away. For example, when I purchased my new laptop, I could get about three hours of battery life; now, I'm looking at

about an hour and a half. To get the best performance from your laptop battery, particularly Nickel batteries, follow these practices:

- » **Fully charge and discharge a new battery or a battery that has not been in use for a while.** Completely discharge a battery to allow it to charge to its full potential. To discharge a battery, power on the portable computer without having it plugged in and leave it on overnight (or longer, if necessary) until the battery power is 100 percent used. You can then recharge the battery by using the AC adapter. Be aware that you need not do this for a Li-Ion battery.
- » **Regularly charge and discharge batteries completely every two to three weeks to keep them healthy.**
- » **Keep batteries clean.** Cleaning the contacts with a cotton swab and alcohol helps maintain a good connection between the battery and the portable device.
- » **Don't leave batteries dormant for long periods of time.** Be sure to use the battery every few weeks and you should fully discharge and charge a battery at least once every three weeks.
- » **Store batteries well.** Be sure to store batteries in a cool, dry, clean place away from dangerous elements, such as heat and other metallic objects.

## *Changing batteries*

A number of laptop users find it useful to purchase an additional battery to keep charged and then switch that one for a battery losing its juice from use. I don't know how many times I've been on a five-hour flight when an hour and a half into the flight, my battery loses its charge. In this example, it would be useful to have another battery that I could switch to.

To change a battery on a laptop, power-down or hibernate the laptop and turn the laptop over. You will notice a spot on the bottom of the laptop where the battery is placed. It will most likely have a battery symbol beside it, with a lever that you slide to release the battery from its slot. Remove the old battery, lightly place the new battery in the slot, and then clamp it in place by pressing down (as shown in [Figure 6-2](#)).





**FIGURE 6-2:** Replacing a battery on a laptop system.

## *Power-management features*

Laptop computers include power-management functions that make the laptop “go to sleep” when there has been no input from the keyboard or mouse for a period of time. When the computer is in sleep mode, it still runs, but power-drawing features like the screen and hard drive are suspended until you “wake” your laptop by pressing a key.



**TIP**

Powering-down the screen and hard drive when you’re not using them helps preserve battery life.

## *APM and ACPI*

Two power-management standards that have come out over the years are Advanced Power Management (APM) and Advanced Configuration and Power Interface (ACPI). These power-management standards have a set

of features that allows the system to conserve power, again resulting in less battery usage for laptop systems.

APM and ACPI are designed to accomplish the same goal, but ACPI is the newer standard of the two and is what most systems support today. APM was implemented as an application programming interface (API) in Windows, which allowed developers to call a library of code that controlled the power management features of the laptop. ACPI was implemented a little differently; it is a set of BIOS routines that control the power management features, which means that to configure ACPI, you make changes through CMOS.

You should know that nowadays ACPI is almost universally used in business- and consumer-class computers.

### ***Configuring power management***

A number of power management features are available to laptops to help conserve the life of a battery and to the desktop computer to simply help conserve power consumption. The following sections list popular power-management features.

### ***STANDBY, SLEEP, AND SUSPEND***

Placing a system in *standby mode* cuts power from peripheral devices (such as the display or hard drive) but maintains power to critical components (say, memory) so that the current work is not lost. *Standby mode* is the term used in Windows; *sleep* is the term used for this low-power state in Windows 10. Another term for this power state used by vendors is *suspend*.



**FOR THE  
EXAM**

*Standby mode, sleep, and suspend* are interchangeable terms for the A+ certification exams.

You can place a system in a standby, or sleep, state automatically or manually. A system can be placed in standby automatically triggered by a certain amount of time when the system has not been used. This is as “idle

time” and is configured by using the sleep timers in the Windows Control Panel.

To change the sleep timers in Windows 10, follow these steps:

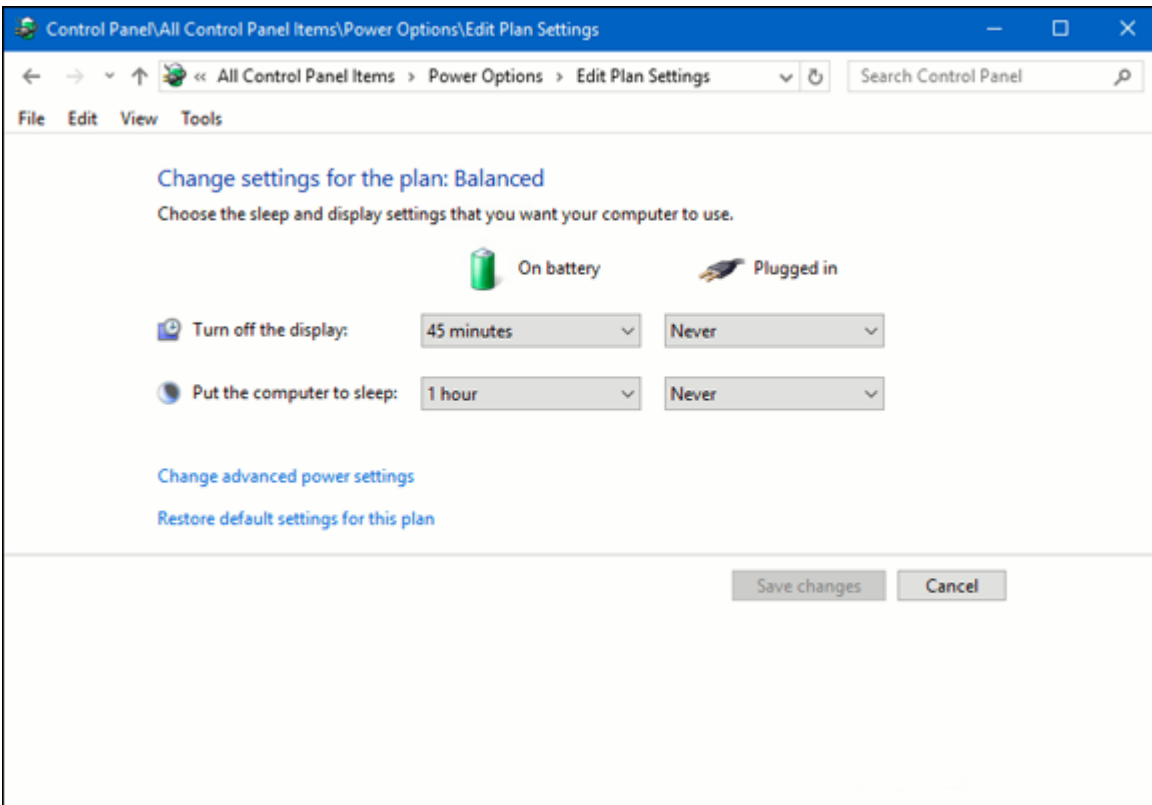
1. **Choose Start, type sleep, and select the Power & Sleep settings search result.**
2. **In the Power & Sleep settings panel, click Additional power settings.**

The Windows 10 development team has been gradually (stress *gradually*) migrating settings from the classic Control Panel to the Settings app. With power options, I suggest we go “old school” and use Control Panel.

3. **In the Power Options Control Panel, click Change plan settings.**
4. **In the Change settings for the plan dialog (shown in [Figure 6-3](#)), adjust the Put the Computer to Sleep: property.**

Note that you can adjust sleep values for when the laptop is running on AC power or battery.

5. **Click Save Changes to put your new options into effect.**

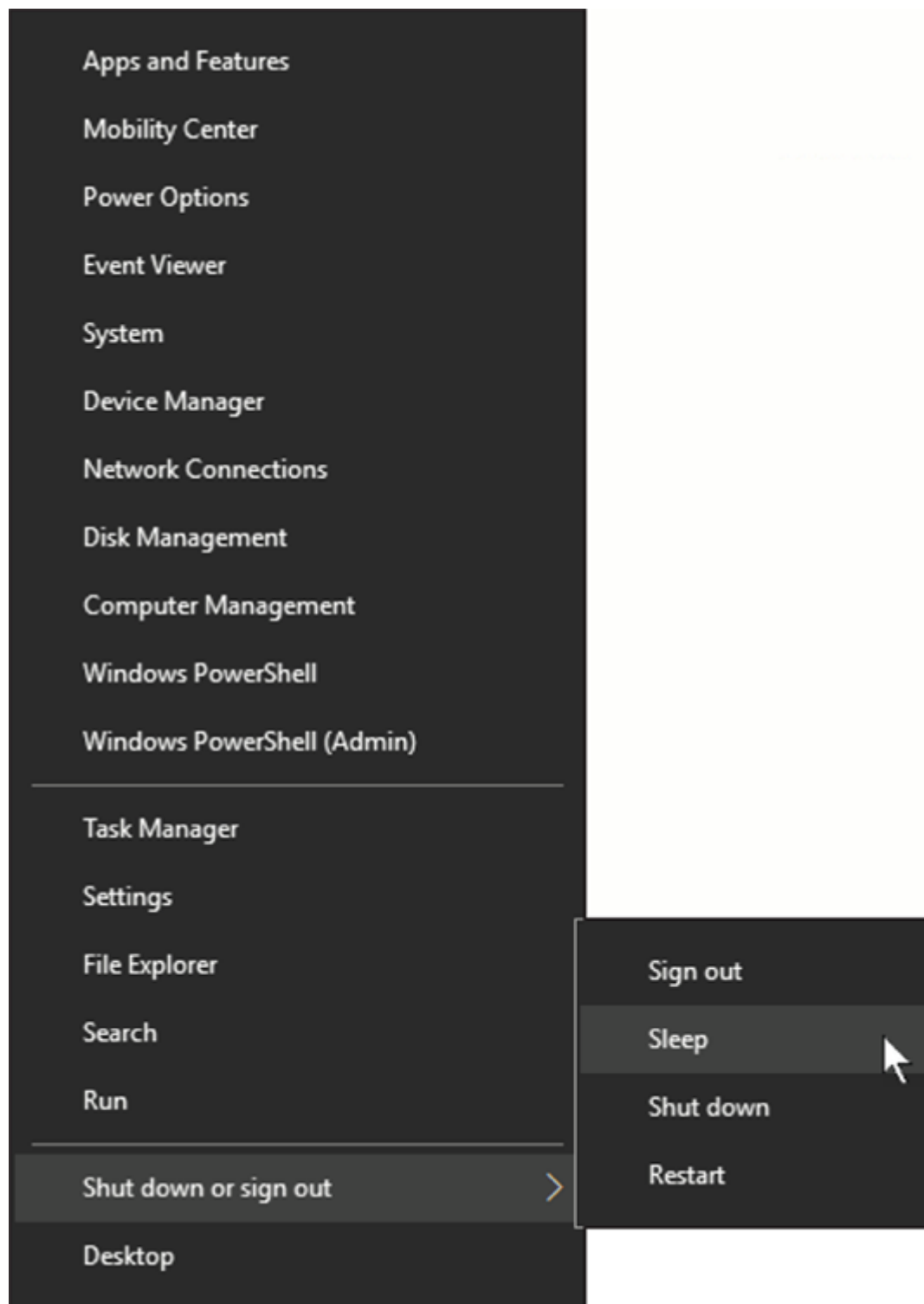


**FIGURE 6-3:** Configuring sleep timers in Windows 10.

Windows makes it convenient to set power-related options. The OS does this by aggregating power options into a power plan.

You can place a system in standby state manually through a number of different means. The following outlines some popular ways to place a system in a standby state manually:

- » **Start button:** Choose the sleep option from the Start button in Windows (see [Figure 6-4](#)) to place the system in standby mode.
- » **Closing the lid:** Through the Power Options in Windows, you can specify to place the system in sleep mode when the laptop display is closed.
- » **Standby button:** Most laptops have a Suspend or a Standby button that you can choose to place the laptop in standby or sleep.



**FIGURE 6-4:** Choose the Sleep option from the Start menu in Windows 10.

## ***HIBERNATE***

You can place a system in hibernation if you need to quickly shut down the system. The hibernate feature copies the contents of memory to file on disk so that current work is not lost; then it cuts the power to the system. When you resume the system, the contents of the hibernate file are copied from disk to memory, and your screen appears as it was when you went to hibernate mode. Windows 10 supports a hybrid sleep function, so that when you put the computer to sleep, the contents of memory are written to the hibernation file; this gives you the benefit of being able to resume your computer if power is lost during the sleep process or allows for instantaneous hibernation if the need arises.

### ***WAKE ON LAN***

Another term on the A+ certification objective list that you need to be familiar with is Wake on LAN (WoL). *WoL* allows you to bring a system out of a sleep state by sending a special message to the system across the network.

This special message — the Magic Packet — has a target address of the MAC address of the system that you want to wake up on the network. The Magic Packet has the broadcast address of FF FF FF FF FF FF placed in the *payload* section of the packet (the data portion of the packet), followed by the target MAC address of the system you are trying to wake up 16 times. Instead of you figuring out how to craft your own packets to wake a system through WoL packets, a number of tools are available for download, such as Depicus tools at [www.depicus.com/wake-on-lan](http://www.depicus.com/wake-on-lan).

To wake your system up via WoL, your system BIOS must support the feature, and you must have the WoL option enabled in the CMOS. For more information on configuring CMOS, check out Book 2, [Chapter 4](#). After the system has the option enabled, you can then power up the system remotely by using a free WoL utility available on the web.

## ***Understanding AC Adapters***

An AC (alternating current) adapter is nothing new to anyone who has worked with electronic devices. The AC adapter on a laptop, just like on an electric razor or a PlayStation Portable, supplies power to the battery

to supply power to the laptop and all its components. An AC adapter also recharges the battery so that you can use it when you are on the road. For example, I am writing this text in a coffee shop and running my laptop off my battery, which was charged up last night by the AC adapter. [Figure 6-5](#) shows an AC adapter.



**FIGURE 6-5:** An AC adapter supplies power to the laptop and charges the battery.



**WARNING** Be sure to use only the AC adapter that came with your laptop or one approved by the laptop manufacturer. Although other adapters might fit your computer, the voltage and amperage might not match the laptop and could cause damage.

### *AC adapter problems*

When it comes to AC adapters, there are not a lot of issues that can arise. Two major problems that you will encounter with AC adapters are

- » **Cable problems:** One major issue that can arise when you travel a lot with a laptop is a break in the cable from wrapping the cables. When you have cable problems, it's best to simply order a replacement adapter.

» **DC (direct current) port damage:** Another major AC adapter problem is that the DC port on the back of the laptop can become damaged: for example, when the laptop is not used on a hard, flat surface. A number of people I have talked to with problems with the DC port not holding a connection to the AC adapter use their laptop in bed, resting it on their knees, which bang into the DC port connector. In this scenario, it is best to have the laptop serviced by the manufacturer to ensure the correct electrical parts are replaced.

### *AC adapter troubleshooting and repair*

If you find that you have a broken wire or faulty electrical components, you can attempt to repair the problem yourself. However, unless you have an electronics background, you should probably leave that to the experts and simply replace the AC adapter.

## *Learning about LCD Panels*

Liquid crystal display (LCD), a popular display or screen type found in laptops for many years, is now a popular choice for desktop computers and TV display. LCDs also are popular on watches and other electrical devices.

An LCD has two sheets of material, surrounding a liquid that contains crystals that act as pixels for the display. Each crystal has a red, green, and blue cell that is illuminated by an electrical charge hitting the crystal, which then creates the image you see onscreen. To present the image to the user in a more clear way and to allow the laptop to be used in more brightly lit locations, the display will usually have overall backlighting.

The two major types of LCDs are monochrome and color. The two subtypes of color LCD displays are active matrix and passive matrix.

- » **Monochrome:** The original LCDs were single-color displays that showed blue or dark gray on a light gray background.
- » **Color:** The two forms of color display are active matrix and passive matrix:



- *Active matrix:* An active matrix display, the most popular type of display today, uses at least one transistor per pixel, or crystal, which allows the electrical charge to be held longer on the crystal. This helps to create very crisp images with high resolution. With active matrix displays, the images are clear and easy to view, even from an angle. Because it uses transistors, an active matrix display uses more power than a passive matrix display. Active matrix displays are also known as thin-film transistor (TFT) displays.
- *Passive matrix:* A passive matrix display has one transistor for each vertical column of the display and one for each horizontal row of the display. The electrical signal is sent down the appropriate horizontal and vertical row of the display, and where they intersect is the pixel that is illuminated. Passive matrix doesn't have a transistor per pixel, so it does not use as much power as an active matrix, but it is slower to produce images and produces lower-quality images. Another popular term used to describe passive matrix is *dual-scan*.

Technology in the area of displays is rapidly changing, and while not all the display technologies are used in laptops, [Table 6-1](#) summarizes these technologies.

**TABLE 6-1 Display Technologies**

<i>Technology</i>	<i>Description</i>
Plasma	While never popular on laptops, plasma screens offer excellent viewing angles, excellent motion support, and reasonable power consumption; but they suffer from image burn-in. Size and weight have been the primary reasons that these screens have not been used for laptops.
LCD	Liquid crystal displays come with fluorescent backlighting, supporting good viewing angles, good video motion support, and very little power consumption. Size and power consumption were the main reasons for adoption on laptops.

<i>Technology</i>	<i>Description</i>
LED	Light-emitting diode displays follow the same technology as LCDs, but the backlighting comes from LED lights rather than from a fluorescent source. This allows a reduction in thickness, weight, and power, all making them attractive options for power-miser laptops. This technology also improves color quality and offers better contrast in all lighting conditions.
OLED	Organic light-emitting diodes are the next generation of LED displays. Their lighting sources are based upon a thinner, flexible sheet of LEDs. These displays will be thinner, lighter, and more power efficient, and will allow the building of flexible screens. Because this is new technology, it is more expensive, but it is expected to be substantially cheaper in the future.

## *Handling LCD panels*

Because an LCD is so easily damaged, take care when handling it. The following are a number of key points to follow to keep your LCD panel working well:

- » **Keep the temperature and humidity at acceptable levels.** The humidity should be less than 60 percent, and the temperature should be no more than 40 degrees Celsius (104 degrees Fahrenheit). This means that you should avoid leaving your laptop sealed up in your car on a hot summer day.
- » **Use only a manufacturer-approved solution to clean your LCD.** Consult your owner's manual for a description of what fluid you should use to clean the display.
- » **When cleaning the screen, don't scrub the surface vigorously or touch it with anything that has sharp edges.** To clean the display surface, be sure to wipe the screen gently with a soft cloth and manufacturer-approved cleaning fluid.

## *Connecting an LCD panel to a computer*

The LCD panel is connected to your laptop by small hinges. In real world, you should be prepared to (a) read your laptop service manual very closely; and (b) maximize your patience to perform a screen replacement, because they aren't easy to do.

Let me give you the most general of guidance, however. To replace the old LCD panel with a new one, follow these steps:

1. **For most laptops, press the spring of the hinges gently to detach the old LCD panel.**



**REMEMBER** Always check the owner's manual or contact the manufacturer to find out exactly how the LCD panel is replaced on your laptop.

2. **After you remove the old LCD panel, slide the new LCD panel firmly in place.**
3. **With the new LCD panel in place, close the panel and reopen it to verify that you fixed the LCD panel correctly.**

If it closes and opens easily, you replaced the LCD panel successfully.



**WARNING** Because the LCD panel is the weakest part of the laptop computer, be careful when handling the LCD and even opening and closing the laptop. If you damage the LCD, you need to replace it.

## ***Touch panel displays***

When you use a self-checkout kiosk at the grocery store, or add a contact on your smartphone, or *<fill in the blank here>*, you're using a touch panel display. Touch displays use a hardware layer called a digitizer to accept analog input from the user's finger and translate it to digital code that's understood by the computer's CPU.

Microsoft launched Windows 8 thinking that most consumers would adopt touch panel desktop computer monitors, but that really hasn't been the case. By contrast, most mid-tier and above laptops do have touch-sensitive displays.

# *Understanding Laptop Input Devices*

After you become familiar with a laptop's major components, such as batteries and displays, take a look at the myriad input devices used to get data into the laptop. The major input devices are the keyboard, touch pad, and rubber mouse ball located on the keyboard of some laptops.

## *Laptop keyboard*

The *keyboard* is the most common input device used on both desktop systems and laptops. The keyboard allows you to communicate with the system by converting the keystrokes into corresponding letters and numbers. For information on the different types of keyboards and how they work, read Book 3, [Chapter 2](#).



**FOR THE  
EXAM**

For the A+ exams, be aware that the enhanced 101-key keyboard is the popular keyboard found on desktop and laptop computers today.

## *Maintaining keyboards*

Over time, a keyboard collects a lot of dust and dirt behind the keys. It is important to clean keyboards periodically, and the following outlines the basic steps for cleaning a keyboard:

- 1. Holding the laptop at an angle, use compressed air to blow the dust and dirt from behind the keys.**
- 2. Clean the tops of the keys with a soft cloth dipped in a manufacturer-approved cleaner.**



**TIP**

You can also buy a wet cloth with the appropriate cleaning fluid already applied.

3. **Using a lint-free swab, clean any remaining dirt from between the keys.**

### *Handling keyboard problems*

Like most replicable components today, replacing a keyboard is far more efficient than repairing it. The following steps provide a basic guideline you can use to troubleshoot any keyboard-related problems:

1. **If you are having troubles with the keyboard after replacing it, check that the keyboard is seated correctly by making sure it is snug in the molding.**

2. **Reboot the computer.**

Yes, rebooting does work from time to time! Rebooting the computer reloads the device drivers, which are responsible for controlling the corresponding devices — in this case, the keyboard.

3. **If the keyboard still doesn't work, or if just some keys don't work, you might need to replace the entire keyboard.**

Personally, I find that the keyboard is the first item to go on laptops. Replacing a keyboard on your laptop may be an easy process. Some are held in by a series of retaining clips, while others will require the disassembly of the entire case.

### *Function keys*

Laptop function keys provide the typical use of a function key, such as pressing Alt + F4 to close the current window. However, function keys on laptops also allow you to control features of the laptop.

Many contemporary laptops “overload” the function keys by allowing more than one function per key. For instance, pressing F1 may perform one action, but pressing Fn+F1 may perform another.

The following list offers some popular functions you should be able to find on your laptop keyboard:

- » **Display Brightness:** On a laptop, you can typically adjust the brightness of the display by using the function key (Fn) and then pressing the brightness function button. For example, on my laptop, I use Fn + F8 to increase the brightness and Fn + F7 to decrease the brightness. New laptops may also have a function key to enable or disable an ambient light sensor that will adjust the screen brightness based on the ambient light.
- » **Display Toggle:** If you hook a projector up to your laptop for a presentation, you need to use the display toggle function key to set the laptop to show the output on the projector and on the screen of the laptop. On my laptop, I use Fn + F4 to do this.
- » **Disable Wireless or Bluetooth:** On laptops without a dedicated key to disable WLAN or Bluetooth radios, you may find that a function key has been dedicated to this function. You may also consider checking to see if updated radio firmware is available for download and installation.
- » **Keyboard Backlight:** This is a new feature on laptops, and many systems now support keyboard backlighting, which illuminates the keyboard using LEDs beneath the keys. This lighting system can be turned on or off using a function key.
- » **Volume/Mute:** Function keys may be assigned to adjust the volume up or down, or to even mute the entire sound system.
- » **Sleep:** If you don't have a Sleep button on your laptop, you might have a function key allocated for this purpose. To put my laptop to sleep, I can press Fn + F5.
- » **Cellular on/off:** For laptops with integrated cell network connectivity, toggle the radio.
- » **Touch pad on/off:** I habitually disable my touch pad when I use an external mouse with my laptop.
- » **Screen orientation:** Portrait versus landscape mode.

- » **GPS on/off:** Enable or disable on-board global positioning system (GPS) if the laptop has this capability.
- » **Airplane mode:** Single toggle to disable all WiFi, cellular, and Bluetooth radios.
- » **Rotating/removable screens:** For laptops that double as tablet devices.



**TIP**

When troubleshooting keyboard issues, make sure that you are not supposed to use a special key — such as Fn or Alt — to go with the keystroke.

I'd like to say a bit more about rotatable/removable screens. First, the screen rotation can often be undertaken in software in addition to in hardware. For example, some tablet devices have software controls to shift the screen orientation between portrait and landscape mode to accommodate different usage/reading styles.

So-called “convertible” laptop computers have a hinge on the monitor that allows the user to swivel the physical display to the back of the device. This effectively converts a laptop into a tablet, albeit a thicker one. Some convertible devices allow you to detach the display from the chassis and keyboard altogether.

Of course, it's crucial that you read the user manual that accompanies these laptops to ensure you don't push when you should pull, or twist when you should turn, and so forth. No need for unnecessary warranty claims!

## *Pointing devices*

Two other major input devices are the touch pad and the mouse ball, which are both responsible for controlling the mouse pointer on the laptop. Most laptop users use a normal mouse with their laptop by connecting the mouse to either a USB port or over Bluetooth pairing.

If you don't want to use a wired USB mouse with your laptop, you will typically control the mouse pointer by using a touch pad or a mouse ball.

### ***Touch pad***

A touch pad, as shown in [Figure 6-6](#), is a very common component found on laptops. It is a small, rectangular surface at the front of the keyboard. To use the touch pad to control the mouse pointer, drag your finger over the surface; the mouse pointer moves in the same direction.



**FIGURE 6-6:** Use a touch pad to move the mouse pointer.

Below the touch pad are two or three buttons, which act as traditional mouse buttons. With most laptops, you can tap the touch pad instead of clicking the left button to perform a “click” operation, and you can tap the touch pad twice to double-click. If you find that the touch pad does not react to the tapping, have a look in the driver CD that came with the laptop to see whether a driver needs to be loaded for the touch pad.



Most laptops also have a button that can be used to turn the touch pad on and off. This can be useful if you're going to use a USB mouse and don't want the touch pad to interfere when you accidentally rub over it, which I find I do with my thumb as I type.

### *Touch stick or pointing stick*

Some (much) older laptops have a small stick, or what I like to call a pencil eraser, in the middle of the keyboard. This is available on models from all major manufacturers. With a little pressure on the pointer in any direction, your cursor on the screen moves. Typically, you will have a set of pointer buttons under the spacebar to act as the mouse buttons. [Figure 6-6](#) also show this pointer between the G, H, and B keys. Notice the two sets of buttons, one above the touch pad and one below. The set of buttons above the track pad are for the track stick, while the set below are for the track pad. For example, my 5-year-old daughter's kindergarten teacher uses a pointing stick with her smart board to annotate projected images onscreen for her students.

Regardless of the type of pointing device that your computer has, it sometimes needs to self-calibrate. When the pointing device is performing its self-calibrating, the pointer will drift to one side or corner of the screen. After running a self-calibration, the pointing device will resume normal operation. This process usually catches people off guard because the pointer moves on its own.

Typically, the need to self-calibrate happens after a certain number of hours, and you might notice it once every few days. If this problem happens more and more often, the pointing device might have an issue, and you might take the laptop to an authorized service depot. Many users will not know what's going on and will fight against the drifting, thinking that something is wrong with the system. However, this is normal operation for these devices — and, thus, a losing battle. As long as recalibration happens only periodically and takes only a few seconds to complete, the computer is working properly. Users should think of it as preventive maintenance.

### *Stylus and digitizer*

A number of portable devices, such as tablet PCs or smartphones, use a touch screen with a stylus pen you use to control the device. (A smartphone gives you features, such as email and Internet access, and has become a popular solution for mobile users.) Some users prefer to use their fingers with touch-sensitive devices, while others like the “old school” feel of a pencil-like electronic stylus.

A tablet PC or smartphone may include a stylus and word-recognition software that converts handwriting to text. The stylus works with a special mesh layer on the laptop screen, and its positioning and tracking are controlled by an internal component called a *digitizer*. The digitizer records where the stylus or your finger makes contact with the screen. Problems with the digitizer — evident through tracking or drawing problems — involve a trip to your authorized repair depot. Handwriting recognition — controlled through software — might involve some training of the system (on some systems) to recognize your writing style. If the problem is with recognition, you might need to retrain the system.

## *Laptop Communication Components*

Laptops communicate with each other and with networks in a few different ways. In the following sections, I discuss some of the popular types of communication components found on a laptop.

### *Network card and modem*

The most obvious communication component on the laptop is its built-in Ethernet network card. You use this network card to plug the laptop into a network via a typical UTP cable. Most laptops today ship with 10/100/1000 Mbps network cards that allow for fast data transfer.

You can identify the integrated network card by looking on the side of the laptop for the RJ-45 jack, which looks similar to a telephone jack, only a tiny bit bigger.

### *Wireless network card*

Most laptops ship with a wireless network card as well as a wired network port. The wireless network card built into your laptop allows you to connect to a wireless access point to access the network and Internet without using a physical network cable.

Laptops typically allow you to enable or disable the wireless network card quickly by pressing a button on the laptop. The wireless button on my laptop is in the top-right corner, but I have also seen the button on the front panel near the hard drive and power lights. From a troubleshooting point of view, you want to make sure that the wireless network card is enabled if you are trying to connect to a wireless network.

## ***Other communications ports***

A few other communication devices are popular in laptops today: infrared, Bluetooth, and WAN-cellular technologies. The following sections give a brief overview of each of these technologies. For more on these technologies, see Book 8, [Chapter 2](#).

### ***Infrared***

Infrared wireless communication uses infrared light signals to send data from one device to another. Infrared is popular with TV and VCR remote controls, but as most of us have found out when using the remotes, infrared requires line of sight. *Line of sight* means that nothing blocks the pathway of the light beam between the two devices. If the pathway is blocked, communication stops. Infrared communication is also limited by its bandwidth; it can deliver information at up to 4 Mbps.

### ***Bluetooth***

Bluetooth is a newer form of wireless communication that is often used to connect a portable computer to peripherals, such as a printer on a network. Bluetooth doesn't rely on line of sight because it doesn't send the data as light beams. Instead, it sends the data over a radio frequency and can be used only when the two devices are close together. Bluetooth has a maximum distance of approximately 30 feet, depending on the Bluetooth device class.

*Pairing* is the process of connecting two Bluetooth-compatible devices. For instance, you might want to pair your new wireless earbuds with your

smartphone. The pairing process normally requires the transmission and reception of a PIN code, after which you can test connectivity to ensure the device works as expected.



FOR THE  
EXAM

Bluetooth v5 is the latest version of the Bluetooth standard, and supports data transmission speeds of up to 2 Mbps.

### ***WAN-cellular or wireless WAN (WWAN)***

WAN-cellular technology allows you to use your cellphone to make a network connection from your portable device to a remote location. The benefit of WAN-cellular technology is that you can connect your portable device to your network from anywhere that you can get a cellular connection. To use WAN-cellular technology, you need a cell-capable device, such as a USB or ExpressCard cell card, or a WiFi tethered connection to a compatible smartphone.

### ***Dongles***

A dongle is a corny name for a hardware adapter. The folks in New England may say “You can’t get there from here,” but that’s certainly not the case with regard to computer hardware.

What I mean is that, with adequate research, you should have no trouble finding USB-to-RJ-45, USB-to-WiFi, USB-to-Bluetooth, or USB-to-optical drive dongles. Truly, the “Universal” in Universal Serial Bus is the truth in 21st century information technology.

### ***Basic mobile device network connectivity and email***

Who is going to purchase a laptop or any other mobile device without giving thought to the question, “How can I get my email set up on this thing?” Answering that question involves first putting the mobile device on a WiFi or carrier network. Portable mobile devices like smartphones include radio firmware that works in conjunction with the device’s International Mobile Equipment Identity (IMEI) and International Mobile

Subscriber Identity (IMSI) values on the device's SIM to put the device on a given carrier's worldwide communications network. You should receive PRI baseband updates directly from your carrier over-the-air; these updates often update the device's Preferred Roaming List (PRL).

## *Port Replicators and Docking Stations*

If you use a laptop at the office a lot, you might want to consider using a port replicator or a docking station to get the functionality of a desktop PC from your laptop. A *port replicator* gives a laptop access to standard computer ports by connecting to an expansion port typically found on the back of the laptop. After you connect the port replicator to the back of the laptop or via USB, it provides serial, parallel, USB, keyboard, mouse, and possibly even display connectors, thus allowing you to use those types of devices on the laptop even if the laptop itself does not contain the ports.

A number of companies set up docking stations for their laptop users. A *docking station* acts as a port replicator by having ports exposed from the back of the docking station. The docking station is different than the port replicator in that it also can contain features such as drive bays, network ports, and desktop computer-sized expansion slots. The docking station will be powered from an AC adapter, so that after your computer is attached to the docking station, it will not require its own AC adapter. The connection between your laptop and the docking station is typically through a proprietary connector on the bottom of the laptop.

## *Expanding on a Laptop*

Expanding on a laptop's capabilities usually involves upgrading the system memory or hard disk (which I discuss in the “[Upgrading Your Laptop](#)” section a bit later) or expanding on the laptop's capabilities by adding an expansion card, such as a PCI ExpressCard.

## *ExpressCards*

Most new laptop computers have a slot that looks like a PCMCIA (Personal Computer Memory Card Industry Association) slot; however, this slot is typically an ExpressCard slot. ExpressCard is the current standard, replacing PCMCIA. In fact, the current ExpressCard standard is ExpressCard 2.0. The speeds that are supported on ExpressCard 2.0 slots are equal to those of USB 3.0 devices.

You find two form factors for ExpressCards, either 34 mm wide (ExpressCard/34) or 54 mm wide (ExpressCard/54). While ExpressCard/54 cards are wider, they are actually L-shaped and have the same 34-mm connector. Because both cards use the same connector, ExpressCard/34 cards do work in ExpressCard/54 slots. In either case, the thickness of the cards is 5 mm.

## *Card readers*

You can find a wide variety of options for semi-permanent storage memory. This memory is typically called *flash memory*, and it can retain its data even when no power is available. Flash memory is what makes flash drives, jump drives, USB drives (the stick ones), or whatever you want to call them possible. That same flash memory technology is also implemented on SD, microSD, and most of the memory cards that are used in cameras or portable electronic devices. Finally, all the SSD (solid state drive) hard drives on the market are based on flash memory actually storing the data on the drive. So flash memory is great, because it allows you to store data on small cards that can easily be transferred between devices, or to increase the internal storage on your devices. I actually use a 32GB high-speed SD card to hold a copy of Linux, which I then use to dual-boot my computer; this leaves my internal hard drive (SSD) completely devoted to my main OS.

## *Upgrading Your Laptop*

In the following sections, I show you how to upgrade a laptop by adding components such as RAM and hard disk space. Makes and models of

laptops vary, but the basic concepts of adding and removing components can be applied to most laptop systems today.

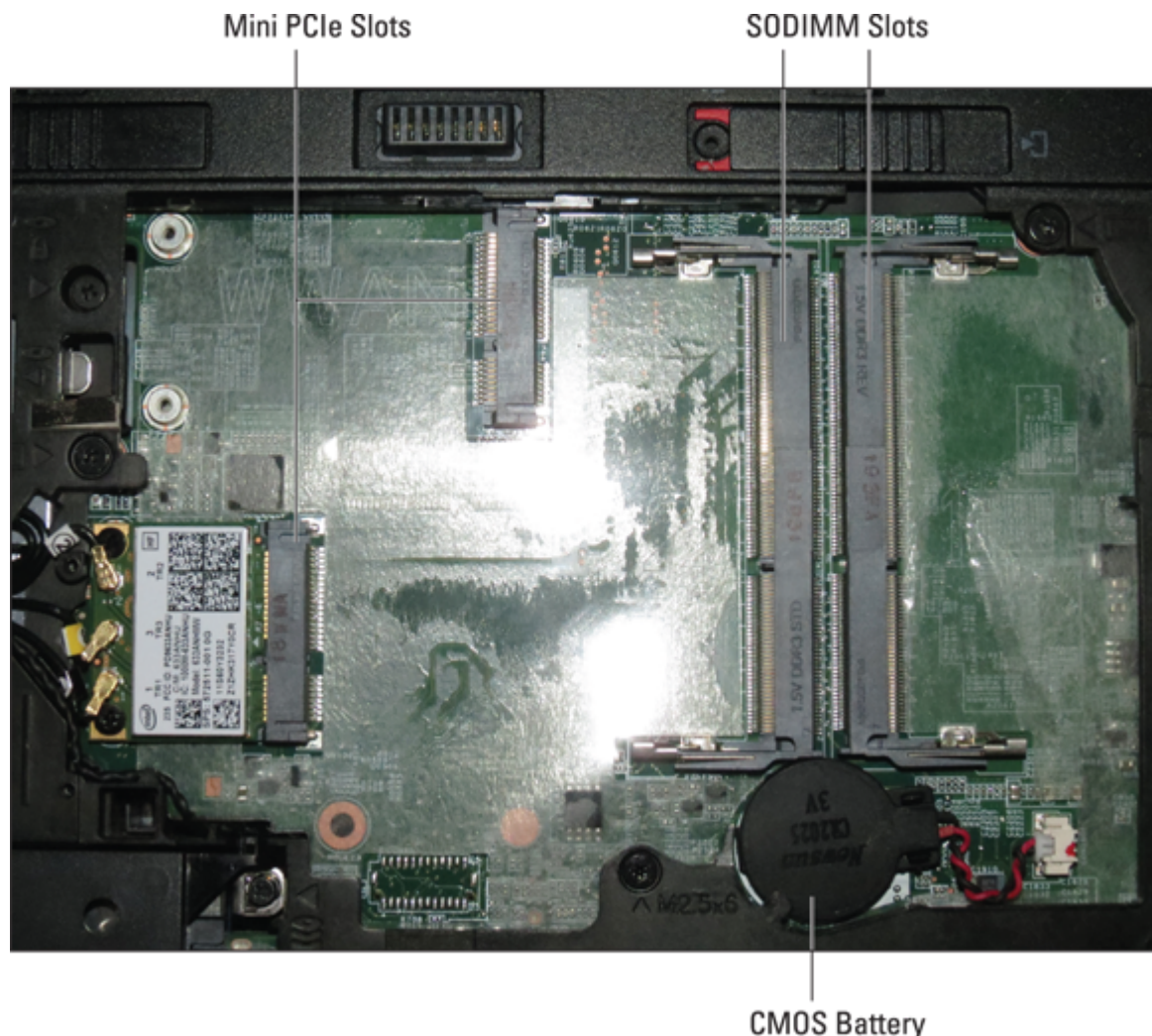
## *Upgrading memory*

To add memory to a laptop, you simply flip the laptop over and find the compartment that holds the RAM. Those are admittedly general instructions — please consult your laptop's service manual for specific RAM slot access details.

This compartment is normally labeled with a symbol of a memory module, as opposed to the compartment that is labeled with what looks like a hard drive. If you are unsure what compartment to open, check the documentation for the laptop.



**WARNING** Remember to ground yourself before touching any internal computer components! After you ground yourself, you can then remove the old SODIMM and insert the new memory module. When inserting a SODIMM into a laptop, be sure to gently place the module in the socket at an angle (see [Figure 6-7](#)) and then clamp it down in place.



**FIGURE 6-7:** SODIMM slots on the laptop to allow more memory to be added to the laptop.

### *Mini-PCI Express (PCIe) cards*

High-performance expansion cards may be added to your laptop through the mini-PCIe interface. These cards are usually found in compartments on the bottom of your laptop. In [Figure 6-7](#), you can see two of these slots, with the leftmost slot already containing an 802.11n wireless card, with three antenna connections. The antennas typically run up behind the laptop screen, providing the best reception when you are using your laptop. The remaining slot is reserved for a WWAN card. The mini-PCIe standard defines this slot as a PCIe x1 expansion slot, but it is also compatible with the USB 2.0 standard. While this standard allows much flexibility in the role of the card that could be installed, on laptops, the main type of cards that are added are wireless communications cards.

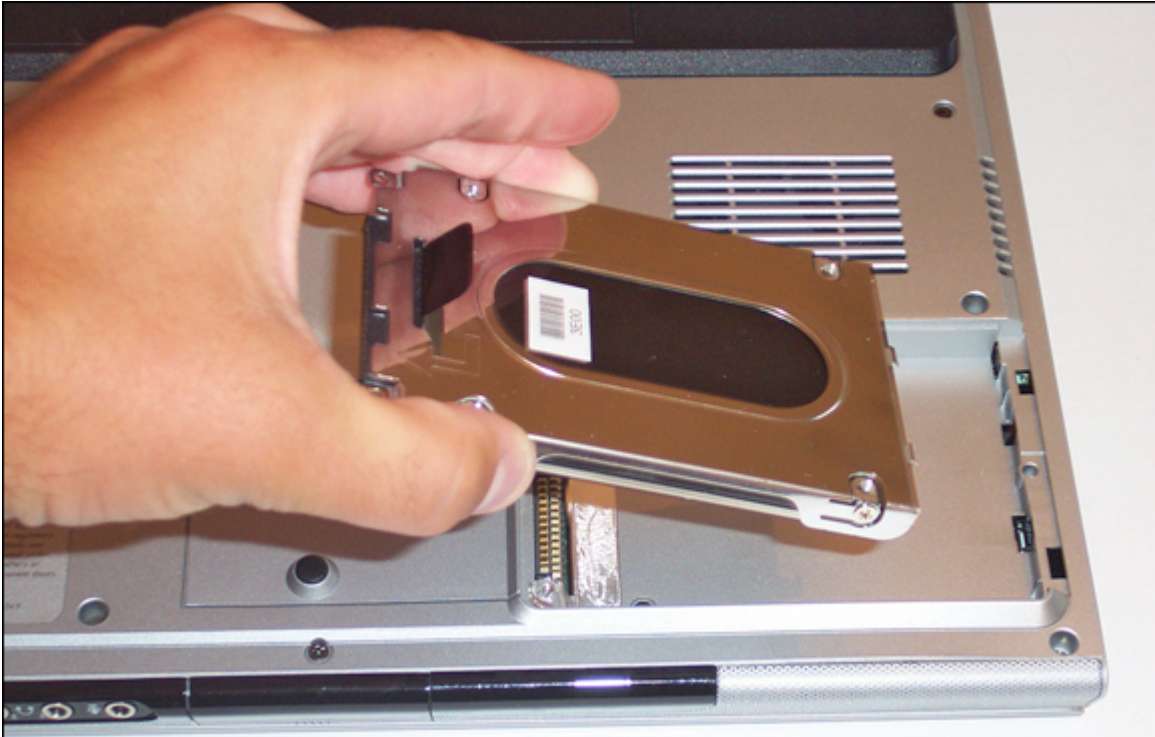


## *Adding hard disk space*

Hard disk space can get eaten up quickly these days when storing media files like videos, MP3s, and pictures from digital cameras. It doesn't take many multimedia files (especially video) to fill up all your laptop's memory.

You can add disk space to the laptop in a number of different ways:

- » **Add an external USB drive.** One of the most popular methods of adding disk space to the laptop is to connect an external USB hard drive to the laptop. This lets you carry the data to a different PC as well.
- » **Get a better hard drive.** On most laptops, you can actually replace the original hard drive with a larger, manufacturer-approved hard drive. For example, you could upgrade from a 500GB hard drive to 2TB. Most laptops have a panel on the back that can be removed to replace the hard drive (as shown in [Figure 6-8](#)). Most desktop hard drives are 3.5 inches wide, while most laptop drives are 2.5 inches. But watch out: Smaller laptops and netbooks may have 1.8-inch drives, so check the size before you buy a replacement.
- » **Use portable unique storage.** Portable unique storage devices include a USB external hard disk, or a flash drive that plugs into a USB port (shown in [Figure 6-9](#)).



**FIGURE 6-8:** Replace the hard drive on a laptop for more storage.



**FIGURE 6-9:** Add storage space by using a USB external hard drive (top) or a USB flash drive (bottom).

## *Replacing your CD-/DVD-ROM drive*

Certain devices on your laptop are made to be changed. Most current laptops come equipped with multibays to make swapping devices easy. My current laptop shipped with a dual-layer DVD burner, but that optical drive is in an easy-to-eject bay, allowing me take the optical drive out and replace it with a new Blu-ray burner or an additional hard drive (installed in a custom drive tray). This makes replacing the drive almost as easy as changing the DVD in the drive.

## *Mobile Operating System Types*

Although I cover operating systems at great depth elsewhere in this book, I thought it wise to make sure you understand the major players in the mobile device operating system (OS) market.

### *Microsoft Windows*

Laptop and tablet devices in a Microsoft world run some edition of Windows 10. In the past, Microsoft experimented with mobile-only Windows versions (that product was called Windows RT), but they eventually standardized on Windows 10 as a sort of universal OS.

Specifically, Windows 10 can run in what's called S mode; this is a highly secure Windows 10 configuration that's optimized for laptop and tablet devices. When a system runs Windows 10 in S mode, you can run only apps from the Microsoft App Store, and can browse the web only with the Edge browser.

### *Apple macOS*

macOS (formerly called Mac OS X) is Apple's desktop OS, which also runs on Apple's laptop models. macOS is based on the history-tested UNIX kernel, and has a super user-friendly graphical environment I've found people either really like or really don't.

Notable is the “walled garden” relationship between Apple hardware and software. Specifically, you can run macOS legally only on Apple-manufactured computers and devices.

## *Chrome OS*

Chrome OS is an interesting operating system. Google built this desktop/mobile OS on its Chrome browser source code. Accordingly, Chrome OS can run only web applications.

The first Chromebooks had hardly any local storage; Google's idea was that the user would access his or her files entirely from the Google cloud. Subsequently, Chromebook designs do have more robust local storage, although the device still retains its "always connected" preference. Chrome OS is available only as a pre-installed operating system on mobile hardware manufactured by Google-authorized partners.

## *Apple iOS*

iOS is Apple's operating system for its mobile device line; this includes the iPhone and the iPad. Eventually Apple plans to fork iOS into versions targeted specifically at iPhone (iOS) and iPad (iPadOS).

Related to iOS are watchOS (for the Apple Watch wearable device) and tvOS (for the Apple set-top box).

## *Google Android*

Finally, Google Android is Apple's biggest competitor in the smartphone OS space. Android offers much of the same wide app ecosystem and user-friendly interface, but also generally greater user control over the device. Android is based on the Linux kernel.

# *Troubleshooting Laptop Issues*

Many issues with laptops require sending them to an authorized repair depot, but you might be able to fix many problems yourself. As a CompTIA A+ Certified Professional, you should also be able to verify which major component of the system is affected. But because laptops are highly integrated systems, many solutions to problems involve a main board or a motherboard replacement. Laptop manufacturers have also made it difficult to get into places that they do not want you to go.

Some standard issues that affect laptops include

- » Power-related issues with external power supplies, batteries, or capacitors
- » External monitors or cutoff switches
- » All the function (Fn) keys
- » Pointer recalibration

When troubleshooting laptop-related issues and when answering A+ certification test questions, you should be familiar with a number of popular troubleshooting best practices:

- » **Verify power.** When troubleshooting laptop power issues, it is best to start with the power supply or power adapter. Verify that either is the correct one for the laptop and that the cables or connectors aren't damaged. You can check the power supply label for the positive lead and use your multimeter red probe on that lead with the black probe on the negative lead to verify the voltage output of the adapter. When troubleshooting power-related issues, such as no power, check whether the LEDs are lighting. You can also try swapping AC adapters to see if the AC adapter is the problem, or if the laptop is. If the AC adapter is functioning, but the battery is not charging, the problem lies with the charging system on the laptop, or more likely, the battery itself. If you have a spare battery, try changing it to see whether that is where the problem lies. If the battery is not holding its charge, it is likely just old and should be replaced. If the battery is new, see whether it can be replaced under warranty.

Less detectable is the fact that some laptops have power issues often dealing with overloaded capacitors or circuits. This can be solved by removing the battery, disconnecting the power, and pressing the power button multiple times (as many as 20 times). Replacing the power cable should then fix this problem. If replacing the power cable doesn't work, though, at least you can test the system without the battery in it so that you can rule out a battery issue.

- » **Remove unneeded peripherals.** Always try to streamline the situation by removing any unneeded peripherals to simplify the

situation. After you get the system operating normally, you can then start adding the peripherals back one at a time to see which device is causing the problem.

- » **Plug in an external monitor.** If you have display issues, such as no display output, try connecting an external monitor and use the display toggle to send the output to the monitor. This allows you to determine whether the video adapter is the problem or the actual LCD of the laptop. While external monitors can solve problems, they can also cause issues with laptops. On many laptops, when the external monitor is connected, it is used instead of the laptop screen. When the external monitor is turned off, the lack of a picture on the laptop can trigger a help call, so always check whether an external monitor is plugged into the laptop. If so, you can use a function key to switch from the external monitor to the laptop screen. The specific key combination to switch between the external and laptop screens varies from one laptop model to another, but often it is F4. Hold down the function key while pressing F4 at two- to three-second intervals to cycle through the display options.
- » **Toggle Fn keys and hardware switches.** Most laptops have three options built into a majority of their keys. Two of those functions are the same as on desktop keyboards and are activated with the Shift key. Laptops, though, also have an Fn key and a series of extra functions identified by additional symbols in another color drawn on the keys. These functions include, but are not limited to, sleep, hibernation, brightness, contrast, battery meter, speaker volume, Print Screen, SysRq, Scroll Lock, Num Lock, Pause, Break, and all number pad functions.

To enable the number pad functions, which are shown in [Figure 6-10](#), do the same thing that you would do on a traditional keyboard: Enable Num Lock. To do this on your laptop, press Fn and Num Lock. This causes several keys on the keyboard to convert from their normal function to act as a number keypad. These keys can be toggled for single keystrokes by using the Fn key as a Shift key. Often, when users accidentally enable the Num Lock, they call you because their keyboard is “broken.” This at least should be an easy fix for you, and

is easy to identify, especially if the keyboard has a Num Lock indicator light. Rather than dealing with this number pad, many users prefer to use a separate USB number pad, some of which do double duty as stand-alone calculators.

Always check the function keys to see whether you can toggle an option off and then on. Be wary of a Function Lock key on your system, which might cause the alternate features of keystroke to kick in.

- » **Change your display settings.** I could not tell you how many times I have watched people struggle to get an external display or projector working with their laptop. An occasional incompatibility exists between screen resolutions, and less often an actual hardware problem. The best thing to do for problem laptops is to refer to the manufacturer's documentation. Typically, the display port on your laptop is active when you toggle the display key — usually Fn+F4 — which cycles through preset display settings.
- » **Check the LCD cut-off switch.** If you don't have any display on the laptop, check whether the display is being sent to the LCD by using the display function key. Also check whether there is a cutoff switch on the laptop that is disabling the LCD. Most laptops also have an LCD cutoff switch that turns off the display when the lid is closed. This switch is usually either a small button at the top of the keyboard or a hole with a mated post on the lid. Depending on the OS settings, triggering this switch might not only turn off the display but also put the computer into standby mode or hibernation. For some laptop models, this switch is susceptible to either being hit or stuck, thereby making the laptop think that the lid is closed.
- » **Verify backlight functionality.** If you have trouble seeing the screen due to a dim display, check that the LCD is toggled on and that the brightness is high enough to see the output. If this checks out, the display backlight could be bad.
- » **Verify connections.** If the screen is flickering, you may have an issue with interference near the display, but more likely it is a loose or broken connection between the display and the video card, or an issue



with the display itself. If a connection issue exists, it will be worse when moving the display back and forth or pressing on the case near the display hinge. Screen flicker may also be caused by the power inverter that powers the backlight system on the display.

- » **Ghost cursor on ghost images.** This does not seem to be much of an issue on modern laptops and LCDs. Early laptops often had issues with screen refresh rates, so much so that moving the mouse quickly could cause it to disappear or leave a ghostly slow-to-disappear cursor where it was. To help with the disappearing issue, Microsoft introduced Pointer Trails or Mouse Trails in the Mouse control panel. This setting actually leaves a series of slow, fading ghost pointers, making it easier to follow a disappearing mouse.
- » **Check the wireless cutoff switch.** I fall for this every time! If you can't connect to a wireless network, the first thing you should check is whether the wireless card has been disabled via the wireless cutoff switch. Most laptops have this switch, and they are designed to give you a quick way to disable the wireless card. Mine is on the front of the laptop, so when I move the laptop on my lap, I end up turning off my wireless. Always check this switch first!
- » **Check the software configuration.** If you have no wireless networking and/or no Bluetooth wireless, check the software configuration. Many manufacturers supply a utility to manage these two wireless signals on your laptop. It is easy to have one or both of them disabled. If you have a wireless tool, you will likely find it in the system tray. If you don't have a configuration tool, a CMOS setting may have been changed. If you have poor signal quality or are constantly dropping the connection, you may have an interference problem. Review Book 8, [Chapter 2](#) for information on managing your wireless signals.
- » **Signs of interference.** If your wireless problems are intermittent, you may be near the outer range of your current wireless solution, or you may be suffering from interference. Sometimes the source of the interference is tough to find. I was sharing a house with another family for two months before I realized that when the phone rang, I lost my



wireless. Refer to Book 8, [Chapter 2](#) for more information regarding wireless interference.

- » **Replace the keyboard.** If your keys are sticking, the problem is likely with the keys or key caps. Laptop keyboards are typically not serviceable, so they need to be replaced. The connection between the keyboard and the laptop is usually through a small ribbon cable. Some laptops will list this as a factory service technician's job.
- » **Numbers print instead of letters for some keys.** This is a popular feature on laptops. Some laptops have a Function Lock key that can be enabled so that the laptop prints numbers when certain keys are pressed. These keys are labeled with numbers on them as well. Another solution to the same problem could be that the Num Lock key has been enabled on the laptop. If this is your case, look for the Num Lock indicator light and the matching Num Lock key.
- » **Replacing plastics.** Laptops will have rigid metals making up their base frame; most of the case material is made from plastics. While plastics are relatively strong and light, they are not overly durable over the long term. Some manufacturers may offer replacements for damaged plastics, especially those that may easily be changed by a user. Many of these pieces may be difficult to replace, so these may be available only to authorized service centers, as they are not field-serviceable items.
- » **Managing speakers.** Internal speakers for laptops are often well situated under layers of case and cables. Changing the speaker may not be difficult for some laptops because it is connected to the main board with an easily removed plug or ribbon cable; what is difficult is removing enough of the case and components to get to the speaker. On some laptops, this is not a field-serviceable item.
- » **Changing the system board.** This is the main component on the laptop computer. Many of the core system components are found on this board, and this means that when manufacturer service technicians are resolving many errors, they will replace this board to resolve the issue. Replacing this core component is not an issue when the system is still under warranty.

» **Replacing the CPU.** Again, this component is not typically replaceable by the user. Most models of laptops come with the option of purchasing one of several different CPUs. Because many CPUs can be installed into the laptop, replacement CPUs can be ordered from the manufacturer and installed. Due to cooling requirements, the CPU is not buried as deeply inside the system, making it much easier to get to and replace than the system board.



**FIGURE 6-10:** Most laptops have a built-in number pad that you activate with the Fn key.



**WARNING** Some components in the laptop are expected to be serviced by the end user (often called field-serviceable parts), while other components should only be serviced by a manufacturer-trained technician. The basic rule of thumb is that if you cannot see how to open a panel or if you need special tools, you should not be doing the task. Most user-serviceable areas have easy-to-remove panels that may not even need a screwdriver. Memory and hard drives are typically accessible for the user.

## *Disassembling and Reassembling Laptops*

This information is true for all equipment that you may choose to work with, whether it is a laptop, desktop, or video camera. But seeing that laptops have a large number of small parts, I focus on them. With laptops specifically, many manufacturers use special screws to complete the assembly. In some cases, they are extremely small TORX-head or Phillips-head screws, or perhaps screws that require a security bit to remove; at other times, you may need specialized tools to separate a case. To keep the lines of the computer clean, some of these screws may be hidden under plastic or rubber screw covers. You must make sure that you have the correct tools for the job. Book 4, [Chapter 2](#) covers many of the tools that you may need to accomplish your job of disassembly and troubleshooting.

If the manufacturer expects that you will be performing a parts replacement job yourself, the company will likely have full documentation for the process. This may come with the replacement part, or even as part of a complete field service manual. Find this out when ordering the part or ahead of time. You can find some hints to documentation sources in Book 1, [Chapter 2](#).

After you get started on the job, you will find that you have a large number of parts and screws. It is best to have a large, clean area in which to work, preferably where your components will not be disturbed. As you move forward with the disassembly, ensure that you document and diagram the components that you remove; this includes the locations of screws and so on. This information will be crucial in the reassembly process. If you are working from proper documentation, you may already have most of this work done for you.

Because you will have many small parts like cables and screws, it is a good idea to have available containers to hold them while working. Plastic part organizer trays are an inexpensive way of maintaining order for your parts. As different types of screws or components are taken off, they can be carefully laid out in your work area or assigned to a bin in your parts tray.

If you are able to stay organized and follow instructions, you should be successful in the service work that you carry out on laptops and other small electronics.

## *Understanding Smartphones/Converged Devices*

Handheld devices are another type of portable device that is very popular today but does not fall into the laptop category. In the past, most handheld devices were limited to a personal digital assistant (PDA) role — such as for maintaining schedule and calendar information. These devices are much smaller than a laptop and use touchscreen technology instead of a keyboard. You typically use a stylus to touch the screen and choose what you want to do with the handheld device. With the improvements in touchscreen technologies, most of these devices can be used with your hand, reserving the stylus for detail work. [Figure 6-11](#) shows a sample of current devices, including an Android-based tablet (including the optional keyboard), an iOS-based iPhone, and a BlackBerry OS device.





**FIGURE 6-11:** A collection of current handheld devices.

Most handheld devices are used to keep track of personal information, such as your contacts or your schedule, but are capable of so much more. Other tasks include Internet browsing, light document editing (word processing or spreadsheets), and running a series of special-purpose applications.

Mobile devices store information to internal flash memory, with additional storage being added through flash memory in the form of microSD or other form-factor cards. These devices are rarely shut down and are put into Sleep or Standby mode between uses, allowing quick device activation when needed. Smartphones, which belong in this category, are always running their call management system.

Because these devices have low power consumption when idle, their batteries can last from a typical workday to several days. Battery life is normally based on device utilization.

Mobile devices support a variety of accessories, connected via special cables or Bluetooth connections. These accessories range from docking stations, to keyboards, to extra battery packs/battery chargers/power inverters, to credit card–scanning and authorization systems; the possibilities are endless.

The trick to successfully repairing built-in laptop components such as inverters, webcams, or microphones is to get your hands on the specific service manual that pertains to your laptop.

Besides giving you step-by-step component replacement instructions, the service manual should also list the specific part numbers; you will need these part numbers when you request replacement parts from the original equipment manufacturer.

Moreover, laptop internal components often require that you have non-standard screwdriver bits, either TORX or perhaps even proprietary to the laptop vendor. Again, you need to perform due diligence, locate the service manual, and open a line of communication with the laptop vendor.

Although most mobile devices (particularly mobile phones and most laptops) include a built-in webcam, this is certainly an accessory that's available separately as well. The same goes for external USB or Bluetooth microphones.

Quality mobile devices also include expansion possibilities like microUSB or miniUSB ports. USB allows otherwise isolated mobile devices to tap into any other USB-compliant hardware.

Most mobile devices support a synchronization function that allows them to be backed up or synchronized with a desktop or laptop computer. The cloud is the new backup and synchronization location. By syncing your device with a cloud-based account, you can then sync your computer with the same cloud location. This allows you to access your data from any device, anywhere in the world. When using devices that have cellular connectivity, you can support over-the-air (OTA) backup of data.

## ***Basic features of mobile operating systems***

All contemporary mobile operating systems include an app launcher and graphical user interface (GUI) that enables users to perform actions on their device. Nowadays we even have virtual assistants like Siri (Apple iOS), Cortana (Windows Phone), and first- and third-party options (Android). Android is a particularly interesting example. Because the Android operating system is open-source, programmers can download the appropriate Android software development kits (SDKs) and build their own Android application packages (APKs). Thus, if you don't like Google's own virtual assistant, you can simply create your own! Finally, mobile devices that include cellular communications capability include emergency notification capability. I'm talking about crucial features like AMBER alerts and E-911, where you need to be get notified regardless of whether, say, you put the smart device on vibrate-only mode or put the OS to sleep.

### *E-readers and phablets*

An e-reader is an electronic device whose primary purpose is the display of electronic books, called eBooks. Although nowadays phablets and tablets have largely supplanted dedicated e-readers, there's still a market for them. For example, my father owns an iPad, but he still strongly prefers his Amazon Kindle Paperwhite for book reading.

"Phablet" is a strange, little-used term that's actually a combination of "phone" and "tablet." These devices, such as the Apple iPhone Plus or the Samsung Galaxy Edge, are bigger than most smartphones, but smaller than tablets like the Apple iPad or Google Nexus.

### *Smart camera*

With regard to the various types of other mobile devices available in the world, I should say just a few words about the smart camera. A smart camera is defined as a digital camera with WiFi and Internet connectivity. Smart cameras make it easy to share your digital snapshots with your social media accounts. Although most smartphones nowadays include smart cameras, the prosumer and professional photographer markets may want to consider digital single-lens reflex (D-SLR) smart cameras to take



advantage of their enhanced resolution and fine-grained control over image dynamics.

## *Looking at the current OS*

In the ever-changing world of mobile devices, it is tough to stay on top of all the current models and operating systems. Luckily, in the current market, the most popular devices fit within the two predominant mobile operating systems:

- » **Android:** This OS is derived from Linux, is owned by Google, and is managed by the Open Handset Alliance — an alliance of several companies, including Google and Intel. The goal of the Open Handset Alliance is to develop open standards for development of software for mobile devices. Due to the open standards, this OS can work on a variety of hardware platforms from various manufacturers.
- » **Apple iOS:** The Apple iOS is a proprietary OS that was developed by Apple and is used by its mobile devices, including iPods, iPads, and iPhones. This is a closed (not open) OS with an established application development process and published development standards. While Apple promotes development of applications on the iOS, it has full control over the development of the iOS, which is limited to use on Apple devices.

Devices running these OSes may take many forms, from the smallest of smartphones to largest of tablets. This line between tablets and phones gets clouded by the fact that many tablets support the addition of cellular cards, turning them into oversized phones, and many of those phones are getting larger. Because netbook-class devices run primarily Windows or Linux OSes, they are classified as small-form-factor laptops.

From the point of view of usability, discarding much of the marketing hype, few differences exist among the various OSes. With varying hardware options, I can expect to see the following features with any mobile device I purchase:

- » **Application source:** Most of the OSes support an online application source, a place where you go to download, install, and update your applications. Android has Google Play, which is the latest iteration of the Android Marketplace; Apple has iTunes and the App Store; Microsoft has Marketplace; and RIM has BlackBerry App World. These application stores have thousands of free applications, games, and media, in addition to ones that you can purchase.
- » **Screen orientation:** While you can view a device in either landscape or portrait mode, unlike monitors that you manually switch between modes, these devices have built-in components to automatically switch orientation. These components include an accelerometer or gyroscope to determine the correct orientation and to be used creatively by applications, such as construction levels or game controls.
- » **Screen calibration:** This task will vary between OS and device. While it was common on older touchscreen devices to need to calibrate the screen to reality, the need to do this on newer devices varies, with most needing so little calibration that software tools are not even provided. When calibration is needed, the software will have you touch several specific locations on the screen and record your deviation from where the OS expected the touch to occur. It then uses this information to create an offset for your use of the device.
- » **GPS and geotracking:** With most mobile devices supporting GPS technology, this tool can add unique capabilities to your phone. Apple and Android devices regularly report phone locations back to Apple and Google. In addition to the report-home features, many apps and tools can use the GPS to report location information to a variety of sources. This makes it easy to keep up on where friends are, or to find your phone after you have lost it. The creative uses of this technology are endless.
- » **Tethering:** There was a time when cell service providers and even smartphone vendors frowned on sharing a device's cellular connection with WiFi clients. However, those days are over. Today you can advertise your smartphone as a WiFi hotspot to any users who

have your administrator-defined password. I use tethering when traveling because my iPad is WiFi only; it's convenient "tunneling" to the Internet through my iPhone's AT&T cellular Internet connection.

- » **Wearable tech:** Apple has the watchOS-based Apple Watch. Motorola makes the Android-based Moto 360. Smartwatches are simply one type of wearable technology. Fitbit, for example, manufactures not only full-fledged smartwatches, but also slimmer fitness monitors that simply track your movement and perhaps your heart rate.
- » **Near Field Communication (NFC):** NFS is taking shape today as a preferred way to handle mobile payments in lieu of the credit card. As of this writing, Apple Pay and Android Pay are the most common NFS-based technologies. NFC offers benefits over the credit card, the chief one being that you can make credit purchases without handing over your card to the teller. Instead, you bring your NFC-enabled device in close proximity to a reader.

From a compatibility point of view, if I have devices with matching or compatible OSes, I may achieve some usability features or benefits, the least of which is a familiarity with the OS. So, if I use an iPhone, my tablet does not need to be an iPad, but if I choose an Android-based tablet, my ability to transfer data and applications between the devices is diminished.

## *Securing your devices*

With the sizes of your portable devices getting smaller and smaller, the need to secure them goes up and up. Even early-generation cellphones had the ability to be locked to prevent people from making unauthorized phone calls (especially when it cost a fortune per minute). But with today's phones and devices, not only can I make calls on your phone, but I can also update your Facebook status, send tweets, transfer money from your bank, or text some pictures to your contact list. Here are some common security techniques that are supported by most smartphones or mobile devices:

- » **Passcode locks:** All portable devices have some sort of software locking mechanism. This is usually found in general or security settings, allowing automatic timed locking requiring a password or code to access the device.
- » **Screen locks:** You don't want some stranger to find your lost mobile device, turn it on, and have immediate access to its contents. All mobile OS vendors include features like timed screen locks in which the device locks after a certain amount of inactivity. More effective are biometric authentication methods such as fingerprint and face protectors.

Adding a second authentication method to a device is an example of multi-factor authentication. For instance, a passcode or swipe lock is something that only an authorized user knows; a fingerprint identifies the authorized user physically, or biologically.

Google Authenticator is an example of a multifactor authentication app.

- » **Remote wipes:** To increase security for lost and stolen devices, the ability to remotely wipe (destroy all information from) a device is crucial. While this has been part of the BlackBerry management from the beginning (through its BlackBerry Enterprise Server), many other smartphones are supporting this feature, either through a centralized management application or a specialized application. Sure, this means that the device will be empty when returned, so hopefully you have a recent backup. But if it does not come back to you, nobody else has the information either.
- » **Locator applications:** Everyone seems to lose his or her phone at some point in time. The old locator trick for a phone lost nearby, if it has a charged battery and the ringer enabled, was to call your own number. The current trend is to work with the GPS in your phone to have it tell you where it is. This involves installing a custom application that registers with a website. By going to that website, you will be given limited access to your phone, if it is still running. This access may give you a remote-wipe capability but also the ability to

display a message on the screen and access the GPS. Through the GPS, you can pinpoint exactly where your device is.

- » **Remote backup applications:** OTA backup is great tool for the busy mobile worker. While I can back up my phone or device on any computer with the management software installed, some people rarely access their computer. Many manufacturers provide cloud-based backup solutions, like Apple's iCloud, Google's Sync, or Microsoft's OneDrive. This means that your phone or device can be backed up automatically, wherever you happen to have a data connection.

Most vendors publish enterprise mobile device management (MDM) solutions to make configuring and administering several mobile devices easier. For instance, Apple has its Configurator tool.

Nowadays, bring your own device (BYOD) is becoming the norm in enterprise business, so admins need tools like Configurator to make their MDM easier to organize.

- » **Failed login attempts restrictions:** As part of the security settings, you may be able to have the device automatically wipe itself when a limited number of failed logins or passcodes occur. Typically, this is set to a high number, like 10, so that it is not triggered accidentally. Having a regular backup is important so that you can restore your data.

- » **Antivirus:** Smartphones and mobile devices are simply small computers. This means that they are capable of having virus software target them. To protect against viruses, you should follow safe computing guidelines and can get extra protection from antivirus software. Depending on your OS, you may find several products to choose from.

- » **Patching/OS updates:** Just as with your desktop OS, as security holes and stability problems are identified with the OS, the manufacturer releases patches. If you are not running a current version of the OS code for your device, you are leaving yourself exposed to security holes and stability problems. Typically, the process to update your device is very easy.

- » **Protective covers:** Given their tendency to drop on the floor and smash into a thousand pieces, you should invest in protective covers for your mobile computer equipment. Some ultra-strength protective covers add waterproofing as an added benefit.

## *Classifying a laptop from a mobile device*

Tablets and smartphones are computing devices, but what criteria are used to separate them from other computing devices, like desktops and laptops?

Here are some of the criteria that you can use to make the separation:

- » **No field-serviceable parts:** Even netbooks give you easy access to a few components such as drives and memory. But handheld mobile devices tend to be pretty closed devices with no parts designed for end users to upgrade.
- » **Integrated OS:** While computers have their OSes installed on a drive, mobile handheld devices have this OS stored on a small amount of internal flash memory.
- » **Touch interface:** The lack of physical keyboard or mouse means that most commands are issued through a touchscreen in a limited-control interface. Since all touchscreens are basically the same, each manufacturer attempts to license and market features in an attempt to make them unique in the market. This includes companies like HTC, which markets TouchFLO and its replacement HTC Sense — which uses innovative movements and controls on Android devices to make typing words on an HTC touchscreen easier and faster by sliding your figure over the letters.

While not licensed technology, multitouch was made popular by Apple, which makes use of multiple fingers touching the screen, thereby *multiple touch* (multitouch), and moving your fingers in gestures to zoom and rotate what is on the screen. Even though there are differences in how things are done on a touchscreen, one thing that is common is touch with either your finger or stylus.

» **Solid state drive (SSD)/flash storage:** When more than a little onboard memory is required, mobile devices make use of flash memory and SSD technology to store information. These storage media solutions consume less power, have no moving parts to damage, and are more resistant to shocks than traditional drives.

While any one of these criteria does not automatically classify your device as a mobile handheld device, if you are hitting most of them, you are safe to classify it as a mobile handheld device rather than a laptop.

### *Synchronizing your data*

While it is important to back up your data, with mobile devices, it is often more important to synchronize your data. When you synchronize — or sync — your data, you copy your data to an alternate location. This process can be completed again and again, each time merely copying the changes that have occurred since the last update or synchronization. Think of synchronization as a two-way copy of changes, so that changes in either location are copied to the other. While some devices can copy data to almost any location, the most common is to have it copied to a computer.

In some cases, synchronization is used as a backup method for your mobile devices. For example, users might back up their remote iPod or iPhone purchases to their computer. In other cases, synchronization keeps two data sources in step with each other. For example, it is common for users to set up continuous data synchronization between Microsoft Exchange and BlackBerry devices. Your options for synchronization will be limited by your device, your synchronization destination, your connection options, and the software options available to achieve the synchronization.

If you can synchronize your data with a computer or a cloud-based solution, you have an easy way to share data between devices and the ability to work on the data wherever it is most convenient.

You may have many types of data stored on your phone or device, but some of that data may be specific to the applications you have installed and may not be capable of synchronization. When looking at an application, I try to find applications that allow me to store favorites or

data to web- or cloud-based solutions — such as NoteMaster on my iPhone syncing with Google Drive. Common data that the phone or device should have synchronization support for include

- » Contacts
- » Programs and program data
- » Documents
- » Email
- » Pictures
- » Music
- » Videos
- » Calendar
- » Bookmarks
- » Location data
- » Social media data
- » E-books

To synchronize your data on your device to your computer, you will need some type of software to be installed on your computer. Most devices ship with the required software that is required to sync the device to your computer. Some solutions include the following:

- » **iTunes:** Apple devices use this to provide basic syncing of your data. This required that you have a Macintosh or Windows computer with a USB or WiFi connection. No solution exists for Linux and UNIX users.
- » **Google Apps:** Android users synchronize their documents and settings with their Google Apps user account.
- » **Manufacturer-provided tools:** Android devices do not have an OS-based sync tool, but some manufacturers, like HTC, supply one with their devices. OS support and requirements vary by manufacturer, but



you can expect that Windows and Mac support will usually be on the list.

- » **Third-party tools:** Because Android does not have built-in sync tools, many third-party sync options are available for Android, some syncing the entire OS while others are application specific.

In most cases, any sync software for your mobile device will support one of three types of connections for synchronization:

- » **USB cable:** This is by far the most common method of device synchronization and backing up.
- » **Bluetooth:** If your mobile device supports Bluetooth, it may support using this connection for synchronization and backup.
- » **Cloud-based/Internet/OTA:** This solution is gaining popularity due to the flexibility and mobility that are involved. This solution synchronizes your device over the data to your own servers to third-party servers and uses that server to synchronize the data to multiple devices.

Many automobiles nowadays allow you to connect your smartphone and access your synchronized data while you travel. This device-auto connectivity takes place via USB or Bluetooth.

## ***Troubleshooting mobile OS devices***

The best advice I have with regard to troubleshooting hardware problems with tablets, e-readers, and smartphones is to rely upon their manufacturer's warranties wherever possible. In fact, I've seen some technicians inadvertently void their customer's warranty by attempting a self-repair rather than submitting a warranty device replacement claim.

That said, CompTIA wants you to be aware of the most common mobile device troubleshooting issues. I list them all (beware, it's a huge list), along with my recommended remedies:

- » **Dim display:** Verify that the brightness slider is set correctly. Perform a soft device reset.

- » **Missing email settings:** Contemporary mobile operating systems normally have a wizard interface to simplify setting up commercial provider email accounts such as Google, Microsoft Exchange, or Yahoo.
- » **Intermittent wireless:** Perform a hard reset. Use a WiFi analyzer.
- » **No wireless or Bluetooth connectivity:** Verify that the WiFi and Bluetooth radios are enabled. For example, the device may be in airplane mode. If you don't know, airplane mode is useful in air travel because passengers are required to disable their radios so as not to interfere with aircraft over-the-air communications.
- » **Cannot broadcast to external monitor:** Verify that the mobile device and the external monitor are on the same WiFi network.
- » **Touchscreen non-responsive:** Perform a hard device reset.
- » **Apps not loading:** Adjust configuration/settings. Uninstall and re-install the affected app.
- » **Poor performance:** Force-stop troublesome apps. Perform a soft or hard reset.
- » **Unable to decrypt email:** Review email configuration settings. Secure email most often uses the Secure/Multipurpose Internet Mail Extension (S/MIME) protocol.
- » **Extremely short battery life:** Submit a warranty replacement claim.
- » **Overheating:** Force stop resource-intensive apps.
- » **Frozen system:** Perform a hard device reset.
- » **No sound from speakers:** Verify that the volume control is enabled and set correctly. Restart the device.
- » **Inaccurate touchscreen response:** Recalibrate display. Submit a warranty claim, citing digitizer issues.
- » **System lockout:** If you don't know the passcode, you may have to perform a factory reset/clean install.
- » **Signal drop/weak signal:** Use a WiFi or cell tower analyzer app.

- » **Power drain:** Force stop troublesome apps. Disable unneeded device features.
- » **Slow data speeds:** Use an analyzer tool.
- » **Unintended WiFi connection:** Verify WiFi settings. Remove unwanted connections.
- » **Unintended Bluetooth pairing:** Verify Bluetooth settings. Delete unwanted pairings.
- » **Leaked personal files/data:** Run antimalware scans. Consider performing a factory reset.
- » **Data transmission overlimit:** Review your usage statistics and make corrections where necessary.
- » **Unauthorized account access:** Back up user data and perform a factory reset.
- » **Unauthorized root access:** Back up user data and perform factory reset.
- » **Unauthorized location tracking:** Review location settings and remove unauthorized connections.
- » **Unauthorized camera/microphone activation:** Verify camera and microphone settings. Consider performing a factory reset.
- » **High resource utilization:** Force stop troublesome apps.
- » **GPS not functioning:** Make sure the device's global positioning system (GPS) is enabled. Consider toggling its state from on to off to on again.
- » **Swollen battery:** This problem occurs most often through manufacturer defect, but can also happen when a mobile device's battery is consistently overcharged. Swap the battery yourself or file a warranty repair issue with the device manufacturer.

## *Securing Mobile Devices*

Let's finish this chapter with a flourish by considering some fundamentals of mobile device security.

### *Trusted versus untrusted sources*

Typically, we think of trusted software installation sources for mobile devices as the device manufacturer or device operating system vendor's own storefronts. For Apple, that would be the iOS App Store. For Android, that would be the Google Play Store.

The advantage of trusted mobile device app stores is that the OS vendor curates its content. This process normally involves scanning submitted apps for sale for malware, determining that the content doesn't violate laws or corporate policy, and so forth.

One concern some businesses have in supporting mobile devices are untrusted app sources that become available once a user jailbreaks his or her mobile device. These untrusted app stores are "wild west" frontiers because the content is typically not scrutinized or tested in any way.

Be careful with jailbroken devices in general, and untrusted app sources in particular. It's one thing to feel you have more control over your mobile device, but it's another to needlessly expand the device's attack surface.

### *Firewalls*

Traditionally, mobile devices have no software or hardware firewall capability themselves. Instead, you rely upon the host network's firewall to protect the device against unauthorized connections.

### *Policies and procedures*

Having your network acceptable use policy (AUP) spelled out literally is a critical action for businesses that support Bring Your Own Device (BYOD) usage scenarios.

With BYOD, employees are allowed to access selected corporate resources from their personal smartphones. The challenge here from an IT standpoint is treading the tough boundary between customer-owned equipment and the need for device security. Again, policies and

procedures make it clear from a legal standpoint what the company's position is, and that the employees are bound by those agreements.

### ***BYOD versus corporate-owned devices***

Some businesses sidestep BYOD and instead issue company-owned mobile devices to its employees. The advantage here is that the company IT team can configure the devices to their hearts' content because, after all, the business owns the devices.

On the other hand, employees are likely to revolt in having to lug around more than one mobile device. Therefore, a more recent IT trend is a compromise that's called COPE, or "corporate owned, personally enabled." COPE takes the attitude of "Here is a corporate-owned mobile device. You are free to make personal calls and install your own apps, but at the end of the day, we have full administrative control over the device."

### ***Profile security requirements***

Mobile devices are normally administered by enrolling in a corporate mobile device management (MDM) platform. Digital certificates are transferred to the device; these encrypt traffic between the mobile device and corporate endpoints.

One or more profiles are also transferred to the managed mobile devices; the profiles implement the corporate security policy by manipulating the settings and environment of the managed devices.

## ***Getting an A+***

In this chapter, I discuss the different components that make up a laptop. These components include the battery, LCD, and keyboard. Be sure to remember the following facts about portable devices when preparing for the A+ exams:

- » The battery in a laptop is responsible for supplying power to the laptop and is charged by the AC adapter.
- » The two types of LCDs used in laptops are active matrix and passive matrix.

- » Most laptops come with built-in ports, such as a network and modem port.
- » To upgrade memory on the laptop, you can add a SODIMM to an empty memory socket located in the laptop.
- » Not all the devices you work with have field-serviceable components.
- » Small mobile devices synchronize your data with computers through various software applications and connection technologies.
- » Major mobile device operating systems include the Apple iOS and Google Android.

## *Prep Test*

**1. Bob calls you complaining that he can no longer connect to the wireless network with his laptop. He has using the wireless network for three months now, and nothing has changed on the wireless network. What would you get Bob to check first?**

- (A) The MAC address settings on his laptop
- (B) That the wireless cutoff switch on his laptop is not enabled or on
- (C) The WPA settings on his laptop
- (D) That SSID broadcasting is enabled on the router

**2. Which battery type is the best battery type for laptops?**

- (A) Alkaline
- (B) NiCad
- (C) Li-Ion
- (D) NiMH

**3. Which of the following components makes the laptop truly portable?**

- (A) Battery
- (B) AC adapter

- (C) DC controller
- (D) PC card

**4. Which video display solution is not used on laptops?**

- (A) LED
- (B) LCD
- (C) Plasma
- (D) OLED

**5. Which of the following statements is true for mobile OSes?**

- (A) The Android OS is an open software operating system.
- (B) BlackBerry devices are capable of downloading applications from the Apple App Store.
- (C) The Apple iOS is an open software operating system.
- (D) Both A and C.

**6. What does LCD stand for?**

- (A) Liquid crystalline display
- (B) Liquid crystal device
- (C) Logical crystal display
- (D) Liquid crystal display

**7. Which statements are true for an active-matrix LCD? (Select all that apply.)**

- (A) It is slow.
- (B) It displays dull images.
- (C) Each pixel is supported by its own transistor.
- (D) Images are easy to view from angles.
- (E) It displays low-quality pictures.

# Answers

1. **B.** Laptop computers have a switch that allows you to temporarily turn off wireless functionality. See “[Troubleshooting Laptop Issues](#). ”
2. **C.** Li-Ion batteries are best suited for portable systems because they are lightweight and have a long lifetime. Review “[Different types of batteries](#). ”
3. **A.** The battery is the component that most classifies the laptop as a portable device. Check out “[Identifying Portable Computer Components](#). ”
4. **C.** Plasma displays, due to size and weight, have not been used on laptops. Peruse “[Learning about LCD Panels](#). ”
5. **A.** Android OS is based on open OS standards, specifically Linux, and promotes open software development processes. Peek at “[Looking at the current OS](#). ”
6. **D.** LCD stands for liquid crystal display. Look over “[Learning about LCD Panels](#). ”
7. **C, D.** Active-matrix LCDs produce high-quality images that are easy to read at angles. Study “[Learning about LCD Panels](#). ”



# Book 4

# Maintenance and Troubleshooting

## Contents at a Glance

### Chapter 1: Performing Preventive Maintenance

[Preventive Maintenance 101](#)  
[Using Preventive Maintenance Tools](#)  
[Maintaining Environmental Controls](#)  
[Completing Maintenance Tasks](#)  
[Getting an A+](#)  
[Prep Test](#)  
[Answers](#)

### Chapter 2: Troubleshooting Procedures and Guidelines

[The Art of Troubleshooting](#)  
[Audio and Visual Troubleshooting](#)  
[CMOS, BIOS, and UEFI](#)  
[Hard Disk Drives and Solid State Drives](#)  
[Optical Drives](#)  
[Working with Connected Items](#)  
[Power Supplies and Batteries](#)  
[Getting an A+](#)  
[Prep Test](#)  
[Answers](#)

# Chapter 1

## Performing Preventive Maintenance

---

### IN THIS CHAPTER

- » Understanding the purpose and use of preventive maintenance tools and cleaners
  - » Identifying and applying maintenance techniques
- 

If you are the kind of person who takes your car for scheduled maintenance, you probably have very few problems with your vehicle. On the other hand, if you have repair work performed only when a problem crops up, you risk always having a major component on your car developing problems.

My point is this: Long-term, trouble-free use of any device involves practicing preventive maintenance. Your computer is no different. Performing regular maintenance helps ensure trouble-free use. As a CompTIA A+ Certified Professional, you need to know what maintenance should be done for your computer. This chapter takes a look at why you want to perform maintenance, what tools you can use, and how to prevent problems by controlling the computer's environment and by maintaining specific computer components.

## *Preventive Maintenance 101*

The goal of preventive maintenance is to prevent problems. Repairs — remedial or unscheduled maintenance — are the flip side of the coin. The main reasons to perform preventive maintenance are so that you can

- » **Save time.** Even though it takes time to perform some maintenance tasks, many can be automated (saving time). If a computer is well maintained, you have fewer repairs to make (saving more time), and the user ends up with less downtime (saving user's time).
- » **Save money by increasing productivity.** Time is money. Users with less downtime related to IT activities are more productive. Also, if you're not spending time repairing computers, your time can be devoted to other pursuits that can improve the overall IT infrastructure.
- » **Protect data.** Data is the life of many organizations. A company that experiences a major loss of computerized data has little better than a 40 percent chance of reopening, better than a 50 percent chance of going under within two years, and only a 6 percent chance of recovering and surviving long-term. With these statistics in hand, you can easily see why many companies invest so heavily in backup technologies. In many cases, though, companies do not plan backups, or they forget about the data that resides on desktop computers — even desktop and laptop computers should be protected.
- » **Improve performance.** All computer systems seem to slow down over time, and some simple steps can eliminate these slowdowns.



FOR THE  
EXAM

Although most businesses can equate everything to saving money, do not forget saving time, protecting data, and improving performance.

One of the biggest things people do not do when it comes to preventive maintenance is create a schedule. When I bought my car, I got a schedule of maintenance activities and when they should be done.

Schedules are great, but if people do not follow them, what good are they? In addition to the schedule for my car (and so I don't forget), I also get warning lights in the car that remind me to perform maintenance. In the case of the computer environment, the more processes that can be

scheduled and automated, the better. If you rely on people to do the task, they will invariably forget to do the task occasionally — or regularly — so automate when possible.

The other important point is to not bite off more than you can chew. That is, keep your maintenance manageable because if it is not, you probably will not do it. Planning to do three things and getting them done is better than planning a dozen and getting nothing done.

Although your schedule for tasks will vary from mine, and might be affected by the industry you are in, having a schedule for your tasks is important. If you do not have a schedule, your tasks will not get done. As I mention, schedules vary from one organization to another, or even within an organization. For instance, a computer on a factory shop floor will likely need its internal components cleaned and its vents checked for obstructions more frequently than a climate-controlled office. A schedule will likely have daily, weekly, monthly, quarterly, and annually scheduled tasks. A list of possible tasks includes

- » Scanning for file system errors
- » Scanning for virus and malware
- » Updating virus and spam definitions and emergency boot disks
- » Backing up data and CMOS settings
- » Defragmenting hard drives
- » Removing unnecessary hard drive files
- » Cleaning screens, mice, keyboards and tape drives, and internal and external surfaces
- » Ensuring that external system fans and vents, internal fans, and heat sinks are functioning properly and are free of dirt and debris
- » Checking power protection devices as well as internal and external cable connections



FOR THE  
EXAM

Although lists will vary, at a minimum, you should remember these items on your list of preventive maintenance tasks.

Schedules vary depending on the computer's environment and use, but when looking at this list, you likely already have done some classification of daily, monthly, quarterly, and annual tasks.

With scheduled maintenance, you might have most tasks automated and performed remotely, but you should have an interval during which each computer is visited. Visiting the computer allows you to conduct visual and audio checks. This goes to the *see no evil, hear no evil* axiom. When you are near the computer, you might notice environmental issues, such as piles of paper surrounding a computer, blocking intake and output ventilation holes. Or you might hear a noisy fan that is close to failure. (When fans start to fail, they are often unbalanced when they start up, and then they slowly level out.)

## *Using Preventive Maintenance Tools*

Your cache of preventive maintenance tools should include software and hardware devices. A balanced approach to maintenance includes a good number from each category.

### *Materials and equipment*

For you to effectively perform preventive maintenance on your computer equipment, you need the correct tools with you. These tools include the following:

- » **Compressed air:** Use to remove debris and dust from surfaces you don't want to touch, or to dust small corners.
- » **Computer vacuum:** These vacuums can be used to remove dust and debris from a variety of surfaces within your computer, such as system fans.

A number of companies produce computer vacuums. One of the largest suppliers is Metropolitan Vacuum Cleaner, which makes the DataVac line ([www.metrovacworld.com](http://www.metrovacworld.com)).

- » **Cleaning cloths:** Cleaning cloths should be lint-free. If you use synthetic cloths, take care when you're working with cleaning chemicals because some chemicals can decompose the cloth or bleed out the dyes in them, which might leave residue on the surfaces you are trying to clean.
- » **Cleaners and chemicals:** Most approved cleaners are mild, nonabrasive, and benzene- and ammonia-free. In most cases, using chemicals should be avoided for most surfaces, and either a dry cloth or a cloth moistened with water should be used.
- » **Cleaning pads:** These soft, lint-free cloths are premoistened with mild cleaners. Cleaning pads are usually more of a convenience item than a necessity.
- » **Manufacturer-approved cleaning kit:** Such kits are usually designed for components.



**WARNING** Never spray cleaners near vents, around keys, or on most surfaces (best to just say “never”) of a computer and its peripherals because of liquid damage that can cause malfunctions or electrical arcing.

## *Software utilities*

In addition to the hardware tools listed in the previous section, many software-based preventive maintenance tools are at your disposal, such as

- » **Automatic update tools** for antivirus, antispyware, OS, and so on
- » **Firmware updates**, although these should be applied only to respond to a problem because they sometimes create other problems, some organizations have a policy to always apply all firmware updates
- » **Driver updates**, which can be thought of as firmware updates



**REMEMBER** If you don't have a reason to update, don't apply updates out of hand.

- » **OS-level tools**, such as `defrag.exe`, `chkdsk.exe`, Task Scheduler (covered in Book 6, [Chapter 4](#)), and Windows Backup (covered in Book 7, [Chapter 3](#))
- » **Third-party maintenance tools**, which are often available as packages from large companies (such as Symantec and McAfee) or from smaller, independent companies
- » **Recovery or rescue boot CD**, which you can use to boot up the computer and repair a damaged OS, or rescue data from a nonbooting hard drive

Many companies provide a disc with prepackaged tools running on either Linux or Windows, often for free. SystemRescueCD ([www.sysresccd.org](http://www.sysresccd.org)) is a Linux example.



**FOR THE EXAM** Remember the hardware and software tools used for preventive maintenance.

## *Maintaining Environmental Controls*

In addition to equipment-specific preventive steps, you can take several environmental steps to protect and preserve your computer. This section looks at those factors and elements.

### *Ventilation and airflow*

When discussing equipment ventilation, only two factors come into play: external ventilation and internal ventilation. Poor ventilation can

contribute to higher-than-recommended CPU temperatures or other damage. Components that are affected by these internal and external factors include power supplies; processors; hard disk drives; and motherboard components, such as chipsets and capacitors. To see how your system is performing, most modern motherboards and hard drives provide temperature sensors that can be accessed from software within your operating system.

### *External ventilation*

The largest single variable in the area of external ventilation is actually the ambient room temperature. If the room is not cool enough, your computer will never be cool enough because the computer simply brings room air into the case to cool components, which is expected to be cooler than the air that is currently inside of the computer case. Room temperatures should be between 60° and 75° Fahrenheit (15°–25° degrees Celsius), but try to stay at the low end of that scale. Most computer manufacturers provide a recommended operating temperature range for their computers. If the computers are constantly used at higher temperatures, your failure rate will go up.

Just like extreme heat is bad, so is extreme cold, and many systems are exposed to extreme cold when being shipped to final destinations. If the outside temperature is substantially below your room temperature (especially if it is below freezing), you should let your computer acclimatize to its surroundings before plugging it in and powering it up. The length of time depends on the temperature variation and whether this warm-up is done within or outside of the packing material. If the computer is left in the packaging materials, the chance of condensation (which should be avoided) on internal components is reduced. In addition to condensation, thermal stress can damage the computer if it is heated too rapidly. (This is similar to pouring boiling water into a cold glass — do not try this at home! Cold items tend to be more brittle than warm items.)

Most computer cases (with intake vents to bring cool air into the case, and exhaust vents to expel the warm air) are constructed from metal to dissipate additional heat that is not exhausted. Objects placed around the case can block the vents and act as insulation for the case, preventing



proper cooling of the computer from occurring. It's obvious enough that exhaust ports should remain open to allow heat to leave the inside of the computer, but if intake ports are blocked, the computer does not get a supply of cool air and will overheat. Without thinking, many people stack papers around and on their computers, blocking intakes.

People also push their computers back to free up desk space, thereby blocking rear exhaust ports. The computer placement and surrounding environment should be checked periodically to ensure that no airflow vents are blocked. In addition, many workstation areas built into desks do not take airflow into consideration, with solid doors on the front and only a small cable routing opening in the rear. Avoid placing computers or monitors in any space that reduces airflow to or from the unit.

### *Internal ventilation*

Besides the environment around the computer, you can do a lot inside the case to aid or hinder ventilation or cooling. The rest of this section looks at factors that affect heat inside the case, and what can be done to reduce heat or increase airflow. To start, I should establish what the typical internal ventilation or cooling process is. As I mention in the previous section, most computer cases are made of metal so that internal heat can be dissipated into the surrounding air. Also part of the case design (and some are better designed than others) are air intake areas and exhaust areas. For tower cases of all form factors, air usually comes in from the front (along the bottom) and is expelled at the top in the back (usually through the power supply). Case form factors are examined back in Book 1, [Chapter 4](#).

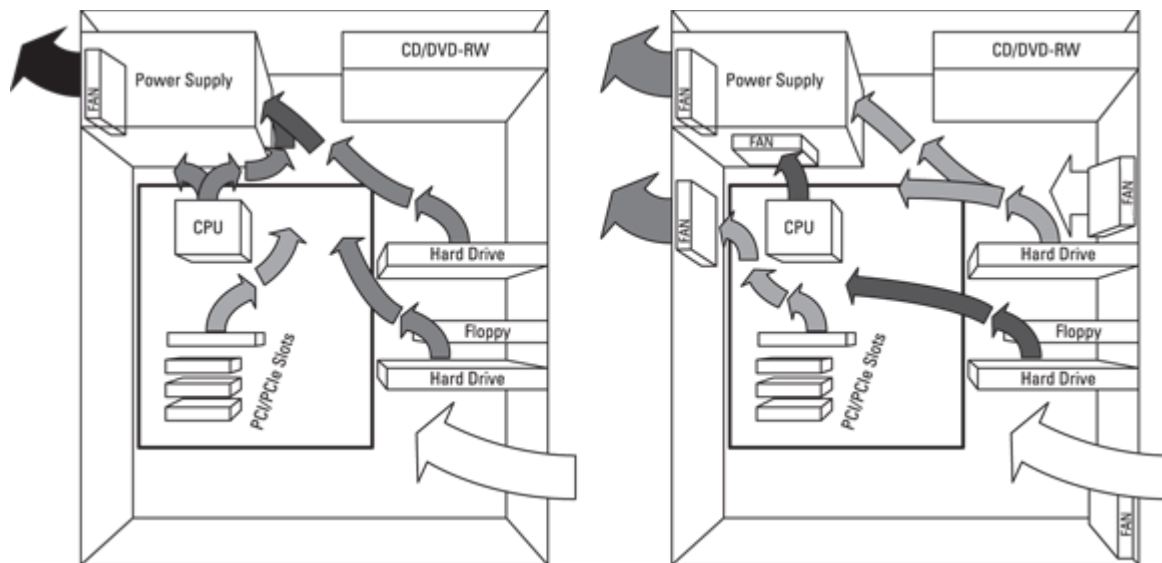
For power supplies without fans, this exhaust is passive. More often than not, though, the power supply has a fan that provides active exhaust. In either case, this situation takes hot air from the internal components and runs that hot air over the power supply components, adding to the thermal stress that the power supply's components already suffer from. To aid airflow, some power supplies have two fans: one external and one internal. When airflow is increased, the expectation is that each cubic foot of air that passes through the space will be cooler. The internal vents or fan on the power supply open either to the front of the case or to the

bottom. When they open to the bottom, they can take more heat away from the CPU.

One popular case design is to have the power supply on the bottom rear of the case and a case fan at the top rear. With the power supply at the bottom rear, it is able to draw in cooler outside air from under the case to cool the power supply components, rather than use the warm air from inside the case. Drawing in cool air through the power supply greatly increases its lifespan; however, drawing in air from under the case can lead to an increase in dust, so clean it regularly.

To keep the airflow going in the correct direction, keep the case cover on and also keep rear expansion slot covers in place. Also make sure that you keep all front ventilation openings clear of obstructions. If you don't do this, the airflow won't go in the direction that the case designer planned.

Many case designers add extra fans and vents to aid airflow. Standard vent locations include an exhaust location on the back of the case below the power supply, which can accommodate a fan that exhausts rising hot air before the power supply has to deal with it. Intake fans are also popular in the lower front of the case, increasing the air intake function. Typical case airflow is illustrated in [Figure 1-1](#), with both a power supply having internal vents opening to the front of the case, as well as an airflow-optimized case with multiple fans to assist in air movement.



**FIGURE 1-1:** Typical airflow in a tower case. The darker the arrow, the warmer the air.

Because the fan on a heat sink typically blows air down onto the heat sink (helping with heat dissipation), another common area for vents and fans is on the side of the case, parallel with the heat sink fan, so that cooler air from outside of the case can be drawn directly to the CPU rather than moving the warmer air existing in the case over the CPU. To augment this airflow even more, some cases also include a funnel on the side of the case to directly channel the air to the heat sink fan. You can find out more about heat sinks and cooling in Book 1, [Chapter 4](#).

Many new liquid CPU coolers make use of a top vent in a case. When not using a liquid CPU cooler on a case with a top vent, fans can be mounted to those top vents to exhaust hot air rising in the case. This make use of the physical principle that hot air naturally rises, and fans can speed that process and assist in airflow.

A liquid CPU cooler makes use of a radiator-type cooling unit with fans, and is mounted on the top vents of a case. This system not only provides CPU cooling without a large heat sink and fan in the middle of the case, but also it also exhausts any hot air directly out the top of the case. If heat is a major problem and this solution makes sense for you, it does give a lot of bang for its buck.

Internal airflow can also be improved by using a larger case, which just has more room for air to move around. There is no bigger heat challenge than taking the newest and fastest multi-core processor (which generates more heat than slower processors with fewer cores) and adding it to a small microATX case with 32GB of RAM and a couple of PATA hard drives. This is a recipe for thermal challenge, especially if noise reduction is also a goal; noise reduction usually means reducing the number or the speed of the system fans. By taking the same components and putting them in a full tower case, the additional air flow from the larger case will reduce the overall system heat.



TIP

Reducing the number of ribbon cables used on PATA devices can also improve airflow. These ribbon cables make little walls within the case that air has to go around. Ribbon cables can be replaced by rounded cables; or, the drives can be replaced with SATA drives, which have smaller cables to begin with. Book 2, [Chapter 5](#) has more information on hard drives and storage options.



TECHNICAL  
STUFF

While the default internal drive connection type would be SATA, PATA devices were used in this example to illustrate that you will encounter challenges, through your choices, or the choices of others. If there is something which impedes airflow, look for an alternative.

In addition to the items already mentioned, wise placement of internal components can help air flow as well. If you're adding two hard drives to the computer, for example, placing them in adjacent bays might seem to make everything look nice and neat. The reality, though, is that such placement also reduces the airflow between the drives, and heat generated by the bottom drive will rise and increase the overall temperature in the top drive. Leaving the one-bay gap allows the system fans to draw some of that heat away from between the two drives, lowering the temperature of the top drive.

## *Humidity and liquids*

In terms of computer maintenance, humidity is a double-edged sword and should be approached carefully. To reduce the chance of electrostatic discharge (ESD), keep a humidity level of 60 percent. To reduce corrosion, though, humidity levels should be as low as 35 percent. Areas that are too damp add to the corrosion of metal components on the motherboard, such as leads for capacitors and the hundreds of metal contact points in the computer. As if corrosion weren't bad enough, condensation is also an issue that can occur if that damp air is also warm

when it makes contact with the cooler computer components. Because water is such a good conductor of electricity, condensation is never good and can lead to major electrical problems. Whenever possible, reduce the computer's exposure to overly humid areas, which can sometimes be done by moving the computer to the next room. You can also extend the cables for the monitor, keyboard, and mouse into the damp environment.

Just as how overly damp environments are bad, extremely dry environments increase the risk of static build-up and cause early wear on capacitors, rubber rollers, and some other components.

In addition to damp environments, spills are another source of liquid problems. In general, avoid using liquids around the computer. If keeping liquids away from the computer isn't possible (who am I to deny you your morning caffeine?), perhaps you can remove the computer from the area of the liquid. You can get special computer cases, keyboards, and accessories that have been hardened to protect them from moist environments, but often at the cost of cooling. To moisture-proof a case, most of the unit — including the ventilation openings — is covered with a rubberized material.

## ***ESD***

*Electrostatic discharge* (ESD) is caused when an electrical charge builds up on one surface, and then that surface comes in contact with another surface that has a lower charge. In most cases, your body builds up a charge when any synthetic materials rub against each other, such as your clothing, or your feet moving across a carpet. Then, when you come close to touching the computer (which is plugged into a grounded or bonded source), the electricity naturally attempts to balance itself out, often jumping the remaining gap and producing a surge of electricity and a spark. The discharge is normally absorbed by the device, and the extra electrical power is drained through the grounding device. However, if the gap were formed while you were inserting a piece of RAM or an expansion card, you could damage the slot or the chipset it is connected to.

Because static is more prevalent in dry locations, increase the relative humidity in the area to reduce the chance of static discharge. When servicing a computer, you can also use antistatic work mats and straps to keep you and the device you are working on at the same potential energy. Even though damage rarely results from small ESD, there is no sense in taking needless chances.



FOR THE  
EXAM

Do not forget the relationship between ESD and humidity. Lower ESD risks by increasing humidity.

### ***The three Ds: Dirt, dust, and debris***

Users are often surprised by how much dust, dirt, and debris collect inside a computer even though the room seems dust-free. Computers collect even more dust when they're placed on the floor, where they essentially act as air filters. In most cases, computers should be cleaned annually. If the computer has to be placed in a dirty or dusty location, though (such as on a factory floor), internal cleaning should be scheduled more frequently. Similar to water-hardened cases (read about those earlier in this chapter), special cases are available for dirty and dusty areas — again, usually at the cost of system cooling.

When system components are clear of dust and grime, they last longer and function properly. On several occasions, I have attempted to install a Windows OS only to get errors during the file copy phase. Normally, this would suggest bad media, but it has invariably been caused by a thick layer of dust and dirt very visibly covering all components. After I use compressed air to get rid of the grunge, the file copy problem invariably goes away. In addition to the dust causing various short circuits, it also causes heat to be retained by the components that are covered in the dust and dirt.

### ***EMI***

*Electromagnetic interference (EMI)*, also known as *radio frequency interference (RFI)*, is caused by rapidly changing signals in electrical

circuits radiating a field around the circuit. This might be caused naturally as part of the circuit's normal operation, or it might indicate a problem with the installation or operation of the circuit. This interference often affects AM frequency bands and other low-frequency devices, such as speakers. If you have been in a boardroom with a speaker phone or radio nearby, you will often hear EMI caused by ring signals being sent to the occupants' cellphones. These signals precede the phone ringing and usually cause a static noise on the speaker or radio. EMI caused by cellphones is why cellphones are banned in certain areas of hospitals — they can disrupt electronic medical devices within about 3 feet.

While EMI can affect wired devices, it can cause similar havoc with wireless devices. Because EMI may cross several RF frequencies, it can affect 2.4 GHz devices, like 802.11b/g/n networks and Bluetooth devices, as well as 5 GHz devices like 802.11 ac networks.

Solutions to EMI include physical isolation of devices, installation of dedicated circuits, power conditioning of incoming power, and replacing devices which cause EMI.

## ***Power, UPS, and suppressors***

*Power conditioning* comprises cleaning or regulating power that is supplied to devices. In addition to conditioning power and reducing EMI, surge suppressors and a UPS (uninterruptable power supply) can provide protection to your computers and electronic devices. If you are using these power conditioning devices, check the status of these devices periodically. Most major UPS have self-test buttons or automatic tests that can be scheduled and reported to administrators, as well as reporting on load levels and battery health. To help UPS and other power protection devices, using dedicated circuits reduces the chance of other devices on the circuit causing EMI, other line noise, power surges, or circuit overloads.

In addition to keeping the power clean and available, grounding equipment is important. All computer equipment comes with *polarity base* plugs (with one side larger than the other), and most have *ground connectors* (the third connector on the plug).



**WARNING** Some users who need extension cords will cheat and get two-conductor cords, thereby removing the grounding facility for their equipment. This should always be avoided because of the risk of damage to equipment from static discharge.

If power interruptions or blackouts are expected, as happens in some areas of the country regularly, computer equipment should either be protected by a UPS or shut down when not in use. This reduces the chance of data corruption from power loss. If electrical storms are a risk, equipment should be protected by a UPS or unplugged, preventing possible damage from a lightning strike. You can find additional information about UPS devices and power conditions in Book 2, [Chapter 6](#).

Aside from the previous points, many people ask, “Should I usually leave my computer on or shut it off?” There are two schools of thought on that, which should not be a surprise. Some factors that affect this decision are:

- » **The convenience of having the device ready to work:** If you visit your computer regularly, you might want to keep it on.
- » **Power consumption:** Running your computer 24/7 will consume more power than shutting it down when you aren’t using it. Many people shut down systems that won’t be used again for 8 or 24 hours. This means either shutting down every night or shutting down just for weekends.
- » **Thermal stress:** Thermal stress happens every time components heat or cool because they expand and contract. This expansion and contraction cause failures to occur. Leaving equipment on for longer periods reduces this problem.
- » **Wear-out:** Most equipment has an expected lifespan measured in hours or days. This rating is the Mean Time Before Failure (MTBF). If components are forced to run continuously, they will hit their usage



limits more quickly, so this problem is reduced by powering items down or having them enter a low-power mode.

The real answer is that you should find the solution that works better for you and your organization.

## *Completing Maintenance Tasks*

With the principles of preventive maintenance under your belt, take a look at what can be done for specific components. This section looks at each of the major components that make a modern computer, and looks at what tasks should be taken to properly maintain each of them.

### *Case and components*

To keep most components in good health, regularly perform maintenance on your systems. The frequency for these tasks depends on the task, with external tasks being performed daily, weekly, or monthly; and internal tasks being performed monthly, quarterly, or annually. The following tasks should be part of your maintenance routine. Make sure that you

- » Optimize airflow both inside and around the case to help prolong the system life.
- » Clean the inside with a vacuum or compressed air periodically to ensure that dust and dirt do not built up on the components or fans.
- » Verify that all the fans function.
- » Check the processor temperature by using internal sensor chips, relative temperature by touch, or a digital infrared thermometer.
- » Ensure that the heat sink and fan are clean and free of dirt and debris.
- » Check the position of expansion cards and removable chips to verify that they are correctly seated.

Newer technology for slots has reduced the chance of chip creep. Still, *chip creep* can occur from thermal expansion and contraction, which happens during the heating and cooling of components. These

heat changes can cause components — such as removable chips — to shift position or work their way out of their mounting clips.

- » Check that external and internal cables are properly seated and connected.



**REMEMBER** Some of these cables can work loose from movement of the case or thermal expansion.



**TIP** If you have systems that use custom CMOS settings (less of an issue these days), ensure that you have a good backup of the CMOS settings. To learn more about CMOS settings, review Book 2, [Chapter 4](#).

## ***Power supplies***

Very few maintenance tasks are associated specifically with power supplies. You should

- » Verify that your power protection devices are working properly to ensure system integrity.
- » Ensure that power outputs are correct. This can be verified with the use of a multimeter or power supply-testing tool. Both of these methods are covered in Book 4, [Chapter 2](#).
- » Verify that the power output is still sufficient if system components have changed.
- » Make sure the fans are clean.

## ***Monitors***

With their lack of moving parts and low number of failures, monitors are often overlooked during the maintenance process. However, even though they are relatively trouble free, include them in your maintenance routine

to ensure that they continue to provide trouble-free operation. At minimum you should

- » **Ensure that the monitor or OS power-saving feature is turning off the monitor properly.** This not only saves power but also prevents image burn-in of a static image onscreen.
- » **Make sure the monitor has proper ventilation.** Ensure that the vents on the unit are not covered. In the days of CRT (cathode ray tube) monitors, the tops of monitors often became storage locations for papers, causing them to overheat. While today's LCD (liquid crystal display) monitors no longer have such an attractive paper filing area, they still generate heat, so ventilation is still important. Try to avoid enclosing monitors in tight spaces and ensure that there is airflow around the unit.
- » **Always check the owner's manual for the correct cleaning solutions for your monitor.** The screens of many monitors these days have special antiglare coatings that are not supposed to be cleaned with standard glass-cleaning products. When in doubt, use a dry cloth or a cloth moistened with deionized water for troublesome spots.



**WARNING** Always apply cleaners to a cloth — not directly to the monitor. This warning should also be applied to any computer equipment that you are cleaning with liquid cleaners.

## *Keyboards and mice*

For keyboards and mice, preventive maintenance includes checking that cables are not damaged by keyboard trays or other external forces. Verify that they are properly connected and have not been pulled loose.

Keyboards on trays can often collect litter that's wiped off the desk, as well parts of meals that some users eat above them. For keyboards, proper maintenance consists of the following:

- » **Prevent spills.** Ensure that food and liquids are kept away from the keyboard's spill area, which is usually about 12 inches (30 centimeters).
- » **Clean carefully.** If a key's surface appears dirty, you can clean key caps with a cloth moistened with a mild cleaner or water. Vacuum around the keys to remove debris between the keys.



**TIP**

Hold the keyboard upside down during this process to keep any debris from falling between the keys.

If debris between the keys is causing key motion problems, use compressed air to blow it out.



**WARNING**

If there is no issue, you might want to leave the status quo because using compressed air could move debris to a position that does cause an issue.

How you keep your mice clean and happy depends on what type of mice you have:

- » **Optical mice:** Verify that the optics are clean and that the surface that it is used on is not too glossy. Some tabletops and mouse pads might not be suitable for optical mice, so add or remove a nonglossy mouse pad as needed for mouse problems. Tracking technology continues to get better with mice, so this continues to be less of an issue as time progresses.
- » **Touch pads:** These devices are typically self-contained and require very little maintenance, but some may have grooves around the edges that may collect dirt. The surface of the touch pad can also accumulate oil from your hands, which can be cleaned with a manufacturer-approved cleaner or a microfiber cloth.

- » **Touchscreens:** You will typically get a buildup of oils from touching the screen with your hands. Unlike non-touchscreens, touchscreens are designed to deal with contact with your hands. Follow your manufacturer's approved cleaning method or use a microfiber cloth.

## *Drives*

Regular preventive maintenance for all types of drives includes verifying that cables are properly connected and that sufficient power is being supplied.

### *Hard drives*

For hard drives specifically, regular preventive maintenance includes

- » Running `chkdsk.exe` scans of your hard drive for errors.
- » Scanning for viruses with an antivirus program, which, together with regular backups of important data, reduces the chance of problems that could affect the integrity of your data.
- » Defragmenting your hard drive to keep disk access at an optimal level; this is not necessary for solid-state drives.
- » Regularly monitoring the temperature and free space of your hard drives and CPU.

You can monitor your hard drives locally with tools like SpeedFan ([www.almico.com/speedfan.php](http://www.almico.com/speedfan.php)), or remotely with SNMP (Simple Network Management Protocol — the TCP/IP device management and monitor protocol) tools like MRTG ([www.mrtg.com](http://www.mrtg.com)) and Cacti ([www.cacti.net](http://www.cacti.net)). These tools gather temperature readings from your *S.M.A.R.T. (Self-Monitoring, Analysis and Reporting Technology)* hard drive, which is incorporated into most new drives. In addition, you can gather S.M.A.R.T. messages from your Event Viewer.

Locally, Windows provides warning messages when hard drive space is very low (less than 200MB).

- » Avoiding vibration and shock. Vibration and shock to the hard drive should be avoided because either can cause substantial data errors.

## DVD drives

DVD drives are optical drives, so occasionally the optical components inside the drive might get dirty. However, this is rare when compared with media problems, which is usually where the problems arise. Cleaning kits for the optical components are available, and you should check with your drive manufacturer for recommended use.

## Storage media

To have consistent access to data you recorded on storage media, you need to make sure that you protect that media.

- » **Scratches and pits:** If your optical media is scratched or pitted to a point that it is unreadable, you might be able to repair or polish it by using a commercial repair kit or car wax.



- » **TIP Deep scratches:** For very deep scratches in optical media, check whether your local video store has a repair service — if you still have a local video store.
- » **Proper labeling:** Optical discs can be damaged by glue found in many types of labels, so a felt-tipped marker is often the safest choice for labeling a CD/DVD.
- » **Body oils:** For all media, avoid physical contact with the media surface. Oil and dirt from your skin can damage the material immediately or over time.

Each type of media has a recommended shelf life, as estimated in [Table 1-1](#); your mileage may vary based on media quality and storage conditions. All media should be kept in a clean, dry, cool, low-light place. If the media is magnetic, keep it away from electromagnetic fields.

**TABLE 1-1** Shelf Life for Recorded and Stored Media

Media Type	Examples	Shelf Life
------------	----------	------------

<b>Media Type</b>	<b>Examples</b>	<b>Shelf Life</b>
Rigid magnetic media	Hard disk drives, removable cartridge drives	15 years
Writable optical media	CD-RW, DVD-RW	5–10 years

## ***Laptops***

Laptops have their own maintenance issues, including screen types, battery usage, charging, storage, and theft.

Before cleaning a laptop screen, check the owner's manual for proper cleaning instructions. Many laptop LCD screens have special coatings or mesh filters that can be damaged if you don't know what you're doing.

With each new generation of laptop computers comes a new generation of batteries, each with its recommended care procedures. Nickel-Cadmium (NiCad) batteries were replaced by Nickel-Metal Hydride (NiMH) batteries, which were replaced by Lithium-Ion (Li-Ion) batteries, which were replaced by Lithium-Ion Polymer (Li-Poly) batteries. The latest generations of batteries do not develop charge memories when not fully discharged between charges, cannot be overcharged, and have a better weight-to-power ratio.

One drawback of lithium-based batteries is that at room temperature, they lose 20 percent of their charge capacity per year, starting at the time of manufacturing. That means that a three-year-old lithium battery will have a maximum charge of about 40 percent of what it was when the battery was purchased. This charge loss can be reduced to 6 percent per year if the battery is stored at 0° Celsius or 32° Fahrenheit, but then the battery needs to be warmed for over 24 hours to return to a usable temperature.

With Li-Ion and Li-Poly batteries, you no longer need to fully discharge batteries. In fact, it is best to keep them topped off; deep discharges can reduce their life.

To keep your battery in tip-top shape, you should let the battery run down (except for Li-Ion and Li-Poly batteries) and perform a charging cycle every few weeks. In general, you can expect to replace your battery every four to five years. If your laptop is going to be used while connected to a

power source, some manufacturers recommend removing the battery, while others have improved charge management systems that will not charge your battery when it is above a specified limit. See your owner's documentation to find out whether this applies to yours.

When moving your laptop between locations, you should use a travel case that is sized and designed appropriately for your computer. This case serves two main purposes: to keep the system free from dust and dirt, and to protect it from shock.

Because laptops are so portable, they are ideal targets for theft, and all come with a lockdown point that you can use with a computer lockdown. A *lockdown cable* — a thick, vinyl-coated braided-metal cable, like the cables used for bicycle locks — needs to be attached to an immovable object. You can see samples of each of these at the Targus website ([www.targus.com](http://www.targus.com)). These devices should be used for a laptop when you are traveling, as well as in your office.

## ***Printers and scanners***

Dust, dirt, and debris tend to be the three big issues with printers. Much of this can be removed with a vacuum, compressed air, and a cleaning cloth, but here are some other cleanliness issues to take into account to keep your printers running smoothly:

- » **Pickup rollers:** Printer pickup rollers can become dirty and should be cleaned with cotton swabs moistened with alcohol.
- » **Print heads:** The print heads on inkjet printers can become clogged and should be cleaned through built-in cleaning procedures on the printer. (See your owner's manual for the exact procedure for your printer.)



**TIP**

If the printer has its print head as part of the ink cartridge, you can also soak the heads in warm water to clear clogs.

- » **Fans and vents:** Laser printers often have fans and vents that should be checked and cleaned out.



- » **Worn components:** Many laser printers have maintenance kits that should be purchased and installed as necessary. These kits often replace components that wear out, such as pickup rollers.
- » **Calibration test:** Many printers also have a calibration routine and a test or diagnostics page that ensures that multicolor print heads are all in alignment and that all print mechanisms are functioning. As part of your maintenance routine, you should print the diagnostics page.

Scanners, like printers, can suffer from the dust, dirt, and debris issues. Scanners tend to have a sealed body, which keeps the internal optics clean, but they usually need to be opened every year or two to clean the internal components. During regular maintenance, only the deck (the glass *platen*) of the scanner needs to be cleaned; use a glass-grade cleaner unless your scanner has a special coating. As always, never spray the cleaner on the surface; apply it to a cloth and wipe the surface. In addition to this issue, scanners usually have a locking mechanism that should be used when moving the scanner, which will keep the scanner properly calibrated.

Because scanners and printers suffer from a build-up of dust and dirt, try to place them in areas that are clean and dust free. I have seen people save money by not purchasing a printer stand, leaving the printer on a carpeted floor, only to pay more than the cost of a stand in additional cleaning and repair services.

## *Getting an A+*

In this chapter, you should remember the following:

- » Perform preventive maintenance to increase productivity and save time and money.
- » Conduct preventive maintenance tasks at scheduled intervals.
- » Standard tools for preventive maintenance include cleaning materials, vacuums, compressed air, and software tools, such as `defrag.exe` and `chkdsk.exe`.

- » Factors that affect computer lifespan are heat and humidity, ESD, dirt, dust, and incoming power issues.
- » Each major component has specific maintenance that can or should be carried out.

## *Prep Test*

- 1. You are working in a factory servicing a computer. The computer is very dirty with oil and grease marks that need to be cleaned. Which of the following is *not* an acceptable cleaner for computer components?**
  - (A) Alcohol and cotton swabs
  - (B) Dry, lint-free cloth
  - (C) Ammonia-based cleaner
  - (D) Cloth moistened with water
  
- 2. You are concerned about a computer that is reporting higher than expected temperatures. You would like to improve the internal airflow to reduce the temperature. Which of the following does *not* help improve computer airflow?**
  - (A) Adding exhaust fans
  - (B) Leaving spaces between devices
  - (C) Keeping vents clear of debris and dust
  - (D) Using ribbon cables where possible
  
- 3. Your manager in the IT department has asked you why you should be performing regular preventive maintenance. Which of the following is *not* a reason to implement a preventive maintenance schedule?**
  - (A) Reduce office temperature
  - (B) Improve performance
  - (C) Protect data

(D) Improve productivity

**4. There has been a lack of adherence to IT maintenance plans.**

**Which two items will help ensure that your preventive maintenance plans are followed?**

(A) Filing completed checklists

(B) Keeping the number of tasks limited

(C) Automating tasks

(D) Purchasing colored index tabs for files

**5. A customer has asked what he can do to better maintain his computer's hard drive. What tools will help with hard drive maintenance? (Choose two.)**

(A) defrag.exe

(B) fdisk.exe

(C) chkdsk.exe

(D) mem.exe

**6. You are servicing a server in a server room. The server room has humidity controls and has been set to low relative humidity. What is one of the problems caused by low relative humidity?**

(A) EMI

(B) PKI

(C) ESD

(D) TCP

**7. You are working on a server in your company's server room. These servers run 24/7. Which of the following can become an issue if you keep your computer running all the time?**

(A) Thermal expansion

(B) Wear-out

(C) Chip creep

(D) EMI

**8. You are working with your archive team who are responsible for proper storage and maintenance of archive media, which includes DVD media. What factors affect the storage life of computer media? (Choose two.)**

- (A) Media length
- (B) Age of facility
- (C) Temperature
- (D) Humidity

## *Answers*

1. **C.** Ammonia- and benzene-based cleaners are too strong for most computer components. Although alcohol is not used as often as dry or water-moistened cloths, it is still acceptable for many computer-related components. See “[Materials and equipment](#).”
2. **D.** Ribbon cables create small walls in the path of airflow and can be replaced with rounded cables to improve airflow in most situations. Review “[Internal ventilation](#).”
3. **A.** Reducing office temperature is something that can help systems as part of a preventive maintenance plan, but it is not a reason to implement the plan. Check out “[Preventive Maintenance 101](#).”
4. **B, C.** Keeping the number of tasks limited keeps the process from becoming unwieldy. Automating tasks removes the need for action on a user’s part, which also promotes having the tasks performed. Filing and indexing physical files will not promote having the tasks completed but can be used to report on what has been completed. Peruse “[Preventive Maintenance 101](#).”
5. **A, C.** defrag.exe and chkdsk.exe are both tools that can be used to perform standard maintenance on your hard drives. Take a look at “[Software utilities](#).”

6. **C.** When relative humidity is too low, there is an increased risk of static build-up and electrostatic discharge (ESD). *Peek at “[Humidity and liquids](#).”*
7. **B.** When devices are running all the time, they can wear out. *Look over “[Power, UPS, and suppressors](#).”*
8. **C, D.** Media’s storage life is greatly influenced by its storage environment, which ideally will be cool, dry, properly lit for archival purposes, and free of EMI sources. *Study “[Storage media](#).”*

# Chapter 2

## Troubleshooting Procedures and Guidelines

---

### IN THIS CHAPTER

- » Troubleshooting major components
  - » Understanding and applying troubleshooting techniques
- 

In the preceding chapter, I show you preventive maintenance routines for your system's devices. Still, no matter how much preventive maintenance you perform, something will eventually go wrong. This chapter continues with the topic of troubleshooting devices — *after* those “somethings” go wrong.

As a CompTIA A+ Certified Professional, you will be required to repair components from many areas of the computer system. This chapter covers the major components found in computer systems and address any troubleshooting steps related to those components.

## *The Art of Troubleshooting*

This section takes a look at the troubleshooting basics you should keep in mind as you start your troubleshooting discovery process.

### *The big swap*

Computer components used to be very expensive. In today's market, though, most components have been turned into commodities and can be purchased very cheaply. Because so many elements are so cheap, replacing components is now more common than repairing them. Because of the reduced cost, you can easily have a small supply of spare

components and test components by swapping in new and reliable components.

Most failures in components occur either near installation or around the expected wear-out period; very few components fail during the normal use period. With technology improvements proceeding at their current rates, technology commonly becomes functionally obsolete prior to hitting the wear-out period for that device. This can be illustrated by CD and DVD drives over the last few years, where most CD drives that fail will be replaced with a CD-RW, CD-RW/DVD combo, DVD-RW, or Blue-ray versions of those drives.

### *Log entries and error messages*

While it may seem obvious to some people, it should not be forgotten that a great place to start troubleshooting is with the actual error message or the content of log files. Far too many times I see an IT professional just randomly start trying things, which may be based on past solutions; but, unless you are sure that what you are doing will resolve the issue, you should review the error messages as one of your initial steps to troubleshooting the problem.

When I get a call telling me that an application will not open, for example, there are many possible causes of this issue, including a bad shortcut, an improper method of launching the application, or perhaps a missing dependency. In many cases, there will be an error message or dialog box, which many people simply dismiss due to the large and friendly OK button, but reviewing that message may give you direct knowledge into the source of the error. Similarly, if there are no error dialogs — and even if there are — you should review any relevant error logs. The Windows OS keeps track of many error logs that are viewable with the Event Viewer application, and many other applications may have their own log files you should review. Like error messages, log files often state the error and sometimes even the cause of the error.

You can read more about Event Viewer in Book 6, [Chapter 4](#).



**REMEMBER** Reviewing log files, event logs, and warning messages should be considered part of your troubleshooting process, as they will often give you the initial indication as to the source of the issue you are asked to resolve.

## *Proprietary crash screens*

When dealing with a major error in an operating system, the display of those errors will vary depending on the OS. Windows, Mac, and Linux will all convey the issue to you in a different manner.

On the Windows OS, the most notorious of all errors is the Blue Screen of Death (BSOD). This occurs when there is a major issue, often with a piece of code that tried to access a memory location used by the OS kernel that the code did not have ownership of. When this happens, the Windows OS immediately stops all code from accessing all memory to prevent possible corruption of any data that resides in memory. In many cases, this attempt to access kernel memory is caused by a driver, as there are few processes allowed to share the processing and memory space used by the kernel.

In the past, this Windows error would display a screen full of hexadecimal code and list the memory locations accessed, memory locations of the process attempting the access, errors, and possible drivers involved. To assist Microsoft in doing deep troubleshooting, a crash dump file containing all the information found in memory would be written to the disk. While Windows 10 continues to do the same process in the background, the outward-facing blue screen includes a frowning emoji and a short message telling you that crash information is being saved to your drive. While not terribly descriptive, this new error is somewhat less intimidating to the users.

Another issue that occurs on all OSes involves a misbehaving process or application running on the computer. This process may be the one you are working with, or it may be a process that is minimized on in the



background, showing no user interaction screens, like a minimized window or a control process such as background updates.

On Windows, this may result in a window not loading, or loading but not drawing the contents of the window. Windows used to use an hourglass to show it was doing something and you should wait, but with Windows 10, the old hourglass has changed to a circle of rotating dots.

On Mac OSes, the wait indicator has taken on a new life with Mac OS X and later OSes — it is now the Spinning Pinwheel of Death (SPOD). While this might just be some homage being paid to Microsoft's long-standing error screen, this spinning multi-colored wheel is called the spinning wait indicator according to Apple's design guidelines. With the most recent Mac OSes, the pinwheel has lost some of its color, but continues to spin to tell you to wait for something to happen. Unlike other progress indicators that may tell you how far along you are in the process via a percentage, the spinning wait indicator does not know how long the process will take, so it spins without a clear indicator of where the end is. This is typically used in all OSes for process like launching an application. The indicator lets you know that it accepted your icon click to start launching the application, but until the application has loaded to a point to fully draw its own window, the spinning indicator lets you know something is happening — or sometimes not happening — in the background. Linux has its own default indicators that vary between releases, but in most cases, it will be a spinning symbol to let you know something is going on.

Regardless of your OS, you will want to look at your list of running processes and close the one that is causing the problem. The problem is likely that your desired process is stuck or failed to load, and needs to be ungracefully terminated; or another process is running out of control and is blocking your desired process from starting up, or making the startup process take a lot more time. If the latter is the issue, you may have problems even getting to a screen that allows you to see the running processes. On a Windows computer you can always resort to Ctrl+Alt+Del to get to a screen that allows you to launch Task Manager, while on the Mac OS you can launch the Activity Monitor, which you may

want to have pinned to your dock for easy access. On Linux the tools you can find on any version of the OS include `ps`, `y`, and `kill`, where `top` will list your top running processes and `kill` will allow you to terminate them. These are both command-line tools; however, there have been many GUI applications written for Linux that give you a similar look and feel to Task Manager and Activity Monitor.

You can read more about Task Manager and other troubleshooting tools for Windows in Book 6, [Chapter 4](#).

## *Physical environment*

To troubleshoot and repair computer systems, you need a large, clean work surface and enough available power connections to power the equipment you are testing as well as your diagnostic tools. You should use antistatic straps and mats for working on equipment and a place to organize your tools nearby.

When doing remote repairs at a client site, you want your travel tools, an antistatic wrist strap, and a clean space to work, although the latter is sometimes difficult to achieve in a cluttered cube farm.

# *Audio and Visual Troubleshooting*

After you conduct your interview to get a list of symptoms (as suggested in Book 1, [Chapter 2](#)), you will often start the first stage of active troubleshooting by looking for audio and visual cues that could be the cause of the described symptoms. This can come in the form of listening to *POST* (*power-on self-test*) errors or beep codes, output from a POST card, or an examination of the physical environment.



**TIP**

When the error occurs prior to when the video sub-system loads, or to help identify the code, you may consider using a POST card or a debug card. This is a card that plugs into an expansion slot and displays boot codes on a simple display as each POST operation is performed. These cards support a variety of interfaces, such as PCI, PCIE, or mini-PCIE.

## ***POST errors***

Each BIOS manufacturer has its own diagnostic codes that identify specific errors. You need to consult documentation for the specific beep codes for your BIOS. Many motherboard manufacturers use codes similar to the original PC POST codes, which are summarized in [Table 2-1](#). If you get only one beep, all is good. In some cases, these beeps are also accompanied by a diagnostic code, which you also have to look up in the BIOS documentation.

**TABLE 2-1 IBM POST Beep Codes**

<i><b>Beep Code</b></i>	<i><b>Description</b></i>
One short beep	Normal POST; system is okay
Two short beeps	POST error; error code shown onscreen
No beep	Power supply or system board problem
Continuous beep	Power supply, system board, or keyboard problem
Repeating short beeps	Power supply or system board problem
One long and one short beep	System board problem
One long and two short beeps	Display adapter problem (MDA, CGA)

In addition to the beep codes, you may also be presented with a numeric code representing the error. You need to consult the documentation for the diagnostic codes for your BIOS, but the general breakdown of the code categories is as follows:

- » **100–199:** Motherboard error
- » **200–299:** Memory error
- » **300–399:** Keyboard error
- » **600–699:** Floppy drive error
- » **1400–1499:** Printer error
- » **1700–1799:** Hard drive error

## ***Connectors and ventilation***

As part of the visual troubleshooting, you will also likely check that intake/exhaust ports and vents are free of obstructions and that cables and connectors are securely attached. As part of the audio troubleshooting, you want to verify that you hear typical sounds coming from your computer, such as fans running properly and hard drives spinning. If the computer is too quiet, it may lead you to fan failures or other sources for your problems.

## ***Warning or indicator lights***

Many devices inside of or attached to your computer will come with status or warning lights. Servers typically have a series of status lights letting you know the state of hard drives, power supplies, RAM, CPU, and temperature. Pay attention to these lights, as they will let you know whether issues exist with components or with the device itself. Some devices will have a limited number of lights or LEDs, and may use patterns to indicate the specific error condition; in these cases, you will need to consult the documentation for that device to identify what the issue is.

## ***More sounds***

You have already seen POST beep codes and noises made by fans as potential notifications of problems with a device. In addition to these sounds, pay attention to other noises that might come from your electronic devices. Hums, grinding sounds, high-pitched whines, or other unusual sounds from a device may indicate that a current or imminent problem exists with the device. These may be loud or quiet noises, and your ability

to hear them may vary from other people's ability. I often state to my wife, “How long has the car been making that noise,” to which I get a “What noise?” Some people are better at picking out abnormal sounds, and while you should not consume your life by examining every abnormal sound, you should at least do some cursory investigation, or acknowledge a deviation from normal. If the noise is loud enough, then anyone should be able to pick out that there is a problem with the device or system.

### *Using your other senses*

Other senses besides sight and hearing can be used to troubleshoot issues with computer systems. These include smell and touch. I will leave taste out as I don't expect that you will want to chew on any of your computing equipment.

When it comes to smell, you may notice smoke or a burning smell coming from the electronics when running. This is typically not a good thing. Valid reasons may exist, such as replaced parts that generate friction burning off shipping oils; but this is more common in the automotive world, rather than in electronics. It is usually safe to err on the side of caution; if you witness smoke or an odor of burning, you have a problem. That problem is likely related to the locations that generate heat or friction; focus on those first.

Heat from electrical current, processing, or friction can generate smoke or a burning smell, but prior to that, you will have heat. All electronics tend to generate some level of heat when operating, and certain problems can cause excessive heat to be generated. Testing for excessive heat is another way to see where the problem may be. Thermometers and touch can be used to identify excessive heat. Many server rooms are equipped with thermometers that can be monitored, and operators can be sent alerts when the temperature is outside a normal range; small-scale heat identification can be used as well.

If you are servicing a computer, excessive dust and lint inside the computer can insulate components, preventing them from staying cool. This lint, like the lint that builds up on electric baseboard heaters over the summer, can cause a burning smell when heated. Some components that

are nearing a failure condition will generate a hot spot, which will eventually overheat and fail; this condition is sometimes seen on stove elements right before failure. The key to remember here, unexpected heat is to be of concern, and that heat may cause smells that may lead you to the source of the heating problem.

## *CMOS, BIOS, and UEFI*

Modern CMOS settings are numerous and easy to access. If you have a computer that requires specific nondefault settings to operate correctly, you want to verify that default settings have not been loaded back onto the system. This can happen if certain jumpers have been moved on the motherboard, the CMOS battery fails, firmware has been upgraded, or you note a strange failure within the system. Improper changes to the CMOS settings (such as boot order, video memory, power options, disk detection, swapping floppy drive letters, and CPU timing) can render the computer unbootable until the settings are corrected. When troubleshooting boot issues, you should verify the boot order in the settings, as this can have your computer attempting to boot to the incorrect device; it may be attempting to boot from the network, an optical drive, a flash drive, or the incorrect fixed drive (HDD or SSD). Adjustments to the boot order can correct the boot issue.



**REMEMBER** If the system settings and time are continually being reset on your computer, remember to check the power on the CMOS battery, as this is the most likely cause.

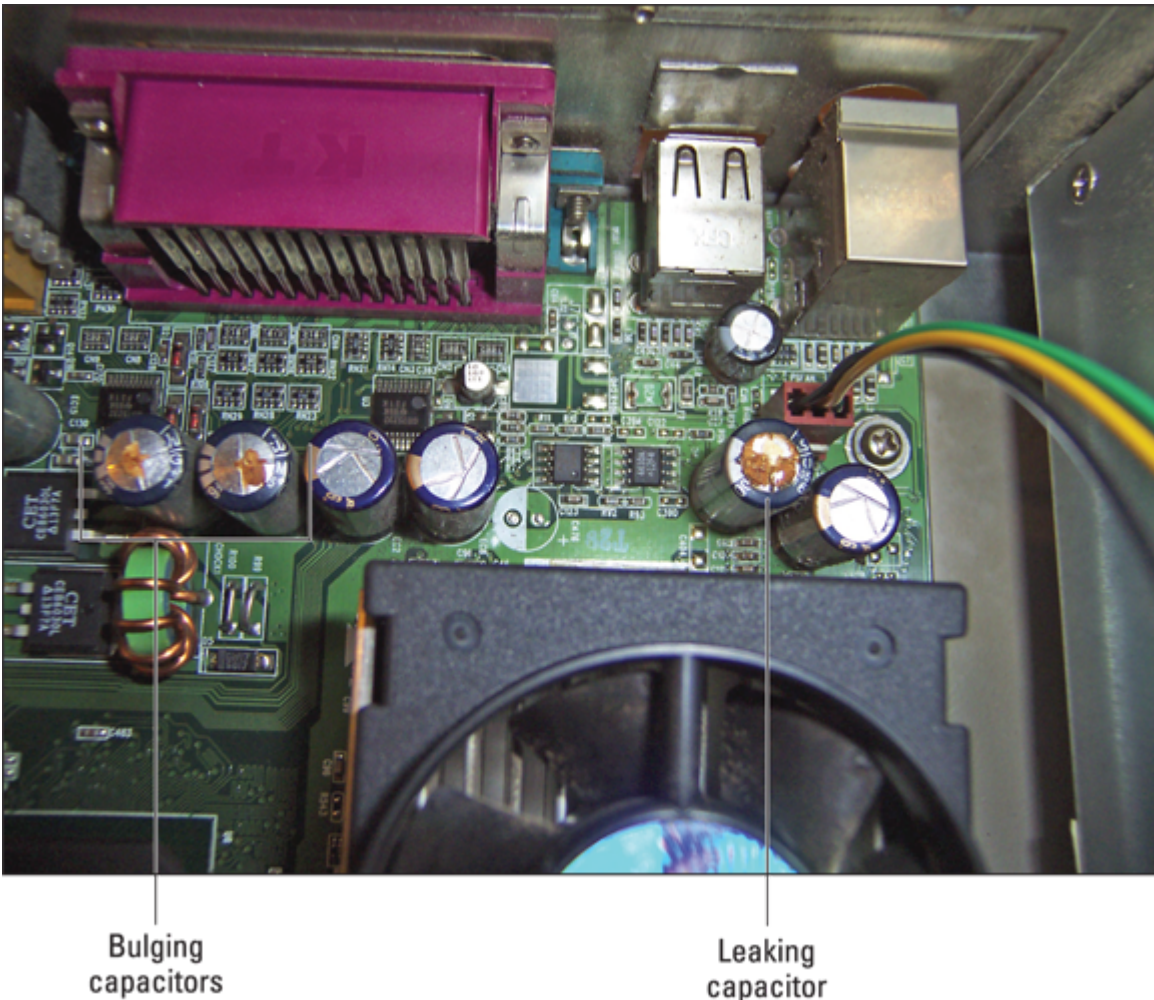
In some cases, you will have a problem with a specific BIOS or UEFI firmware version, and the motherboard or device vendor documents a fix through a newer version of the firmware. If this is the case, refer to the update procedures and follow them. If they give you an option of backing up the current version of the firmware, perform that step as a recovery option.

Sometimes firmware updates can cause more problems than they fix. In some cases, the update is one-way, and you won't be able to revert to older versions. After some upgrades, custom settings need to be reapplied.

Power-saving features in the firmware may allow you to reduce the speed of the CPU to save power and reduce heat. For some situations, this reduction is used as thermal protection when the heat sink fan has failed. If you're looking at performance issues, this is one area to examine.

## ***Motherboard***

Motherboards are made up of many integrated components, and management of these components is done through CMOS settings or by changing jumper settings. You can find specific settings in your motherboard documentation. In addition, you can perform a visual inspection for damage, such as broken connections or capacitor damage (distended or leaking), as shown in [Figure 2-1](#). If you are looking for a failure in a component related to the motherboard, you should also verify that all relevant cables are connected to the motherboard correctly.



**FIGURE 2-1:** Some of these capacitors have damage. Note the residue on the top of the one that has leaked.

## *Processor/memory*

Processor failures are rare but not unheard of. When a processor completely fails, the typical issue will be a blank screen at boot-up, and there will not be a system beep to identify that the system is booting.

In some cases, if failure occurs immediately after installation, the issue may be related to seating of the processor. When the processor is added to the system, a cooling mechanism is added as well, such as a heat sink and a fan. When you install the cooling mechanism, you should use either a thermal pad or thermal gel to improve heat transfer between the processor and the heat sink. If fan or heat sink fan failure occurs, many processors reduce their speed to help reduce heat generation.



Memory errors are often identified during the POST process, when memory is tested. It should be noted that soft reboots usually skip POST tests, so full power cycles (using the power button) should be conducted from time to time. Fan and ventilation problems can also result in memory overheating and generating failures. Other errors occur when technicians unknowingly mix different types of memory, such as ECC and non-ECC memory (covered in Book 2, [Chapter 3](#)), or memory that runs at different speeds.

## *Hard Disk Drives and Solid State Drives*

When you're troubleshooting hard drives, don't overlook the physical problems. Many people dive straight to the software before checking all the hardware. If the drive is not detected or has data errors, you should check the connectors on the drive and motherboard to verify that the cable doesn't have any signs of damage. Sometimes just replacing the drive cable does the trick.

See whether anything might have recently happened that could have caused a shock to the hard drive, such as dropping the computer. Other causes for errors and drive failure include heat problems, so verify drive placement, airflow, and heat dissipation for the drive. Other issues that can cause detection problems are the jumper settings for the drive. If the drive is set for Master, Slave, or Cable Select operation, you could have problems if the setup is wrong for your situation. In some cases, you might have multiple jumper configurations for each setting (as shown in [Figure 2-2](#)), and all should be tried if there is a problem. For complete information about hard drive configuration, read through Book 2, [Chapter 5](#).



**FIGURE 2-2:** Some drives have multiple jumper configurations for the same setting.

The chances of working with PATA on desktop and laptop systems has reduced drastically, which means you will likely be working with SATA devices rather than PATA devices. If by chance you encounter a PATA device, you may have issues with CMOS configuration related to one of the many methods to overcome the base limits of ATA, such as LBA (Logical Block Addressing) mode. Because you will not likely encounter such an issue, I focus on SATA issues.

For SATA drives, both normal and SSD, you will be able to verify that the computer sees the drive by using the firmware settings of your motherboard. If you cannot see the drive in the firmware, then you need to

- » Verify or replace your cabling, both power and data cables.
- » Verify power to the drive by using a power supply tester.
- » Verify the controller port you are using has been enabled.

- » Test the drive in another computer.
- » Test the drive in an external enclosure.

If the drive works anywhere else, then the issue is not the drive itself, but rather something more specific to the computer; perhaps you have exceeded the power availability of the power supply. Another factor to consider is the compatibility setting for the SATA controller; many SATA controllers in desktops support these three modes:

- » IDE
- » Advanced Host Controller Interface (AHCI)
- » RAID

IDE mode operates the controller in backward compatible mode, and was only needed during the industry transition from IDE or PATA over to SATA.

On the software side, you can use `chkdsk.exe` or a similar tool on a rescue disk to test for file system and disk errors if the problem is with unreadable files or an inaccessible disk. If the problem is performance based, checking for disk errors is still a valid step, but you can also check for disk contention on the data bus and possibly move multiple drives to separate IDE/PATA channels or purchase an additional controller.

Running Performance Monitor and monitoring disk counters will tell you whether the disk is being overused and is suffering from contention issues, which can be solved by moving some of the data files that are heavily accessed to an additional hard drive. To choose which data files to move to a new hard drive, look at the actual applications running on the drive.

Other issues affecting drive performance include the type of bus that is being used. To improve disk I/O performance, ATA/66 controllers and drives can be upgraded to ATA/100 or ATA/133 components; SATA 150 controllers and drives can be upgraded to SATA 300; and 5400-rpm drives can be upgraded with 7200-rpm, 10,000 rpm, or SSD (solid state disk) drives. When selecting a new drive, rotational speed, onboard cache, access time, and seek time should all be considered. If cost is no

issue, then SSD is always the correct choice for performance; otherwise it is a tradeoff between cost, storage size, and performance, as SSD drives cost more per MB.

## *Optical Drives*

As with hard drives, the connectors, cables, power, and jumper settings affect how the optical drives work. Optical drives include CD, DVD ROM, and Blue-ray drives, as well as re-writable drives. In addition, problems with optics and alignment can be a factor with optical drives; and a major shock can knock the drive mechanism out of alignment, requiring that you replace the drive. These drives also support analog audio, which makes an analog connection directly between your DVD player and your sound card, allowing audio CDs to be played without requiring transfer of the data through your PATA or SATA data cable. This analog audio cable needs to have its pin configuration verified at both ends of the cables.

Media problems can occur because of media storage or abuse. As I describe in the preceding chapter, some scratches may be repaired to a point that you can recover some or all data from damaged disks. Disk damage from glues, chemicals, or heat may be mostly or entirely unrecoverable.



**TIP**

When booting your computer, CMOS typically stores configuration information including the selected boot device, be it a CD-ROM, hard disk, flash drive, or network. If your computer is not selecting the correct boot device, verify the settings found in CMOS.

## *Working with Connected Items*

While you may see most of these items integrated into a laptop, there are many items which connect to a desktop computer. This section takes a look troubleshooting some of those items.

## *Keyboard and mouse*

Sometimes, keyboard problems are easy to fix. For example, the user enables scroll or number locks, which can be verified by the keyboard's LEDs. Most of the time, though, the problems are a result of damage from abuse or an accident, with the most common accident being spilled liquid. For the most part, these devices can be considered disposable because they cost so little to replace, but they still might require a few troubleshooting steps to identify where the problem lies.

If the issue involves liquids or debris, such as food stuck under the keys, you might be able recover this device with little effort. For example, food and other debris can be blown out with compressed air. However, if the liquid contaminant contains suspended particles (such as sugar or salt) or is acidic, the keyboard is likely a write-off, especially if the liquid caused a short circuit or corrosion has set in. Cables may be damaged by keyboard trays, and both the cables and connectors should be checked for damage. For wireless devices, the batteries should be checked; failing batteries can cause a variety of usage problems.

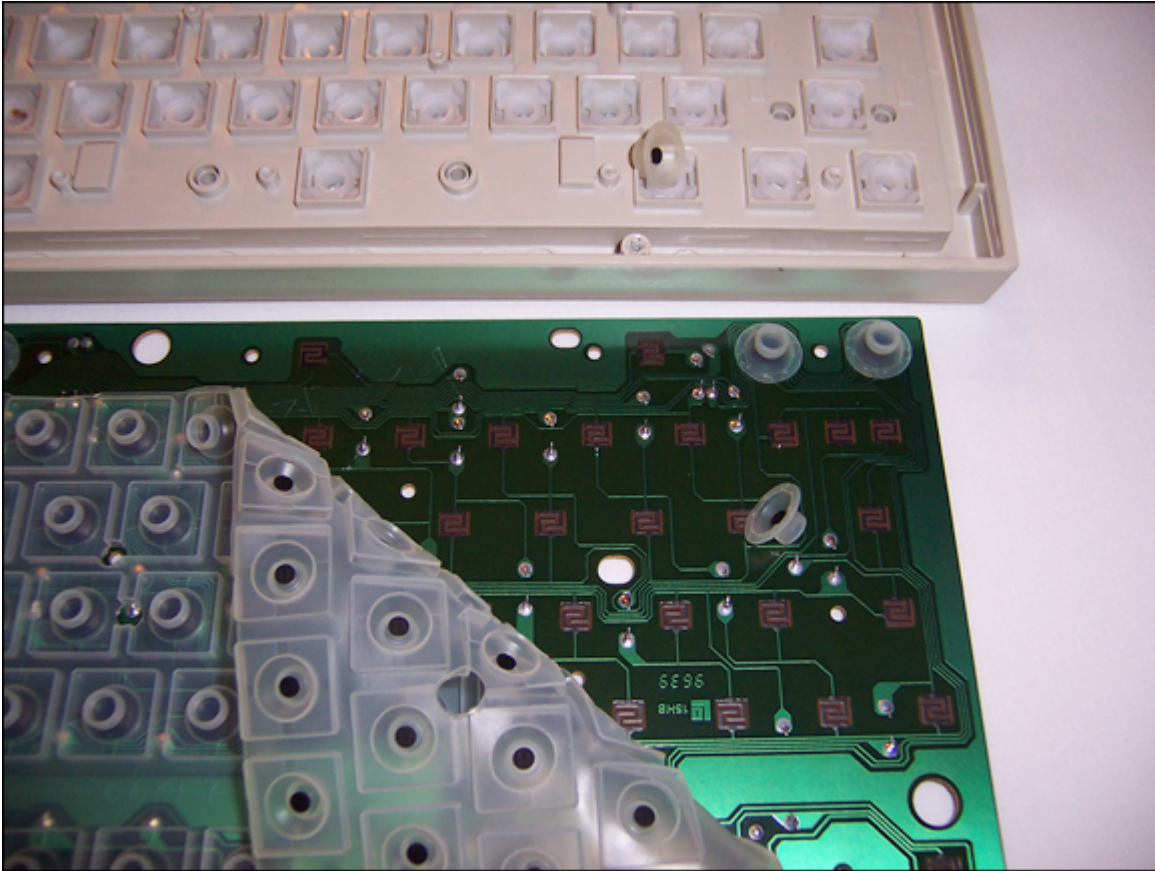
If you have an urge to recover a keyboard with liquid or debris damage, you can soak it in *deionized water*, which is free of particles, and is also electrically and acidically neutral.



**WARNING** If you soak the keyboard in deionized water, the keyboard should be hung to dry for 24 to 48 hours. Do not apply heat to it to dry it faster. Adding heat can cause even further damage to the keyboard.

You can disassemble some keyboard models by removing the keycaps and also the case screws on the bottom of the keyboard. When disassembling a keyboard, remember that it contains a lot of little pieces, as shown in [Figure 2-3](#), and they all have to go back in the correct places. Some keyboards also have springs under each keycap. And in addition to all the small pieces for all the keys, don't forget the circuit board, which can be cleaned with an isopropyl alcohol-based cleaner and cotton swabs or lint-free cloths.





**FIGURE 2-3:** Keyboards can be taken apart and cleaned, but they do contain a lot of little components.

Many traditional style keyboards have removable keycaps. If the dirt is just on the keycaps, remove the keycaps with a special removal tool that has two wires that fit under the key and pull the key directly up. After the keycaps are removed, clean them in a mild cleaning solution and replace them.



**TIP** In general, keyboard repairs are not cost effective because of the time it takes to make repairs and it is far easier to replace the keyboard. It would take an expensive, custom, and not easily replaceable keyboard to cause me to spend any time trying to repair an issue rather than replacing the keyboard.

Tracking problems are the most common ones that occur with mice; with mechanical mice being a thing of the past, you should only have to deal with optical mice. Two factors that affect optical mice are dirt on optics and the surface on which you are using them. If you are using a corded mouse, check the cord for damage and replace the mouse if the issue related to a damaged cord.

## *Audio*

Sound card and audio problems are often related to the connections to the external or internal speakers. Some sound cards and motherboards have additional connections for digital audio using an *S/PDIF* (*Sony/Philips Digital Interface Format*) connection, and others support 5.1- and 6.1-speaker surround sound. When using these types of connections, you should carefully verify the connections against the manufacturer's guide. When working with external speakers or surround sound systems, note that all of them require power to allow for amplification or separation of audio signals, so make sure that the power is plugged in.

One of the big differences between DVI and HDMI is that the HDMI interface also sends an audio stream to HDMI devices, making it great for entertainment solutions. If you are not getting HDMI audio, then you should

- » Verify the CMOS settings to ensure you have disabled HDMI audio.
- » Verify that you are not using a DVI to HDMI converter on a DVI port on your computer; if this is the case, there is no audio signal on the HDMI cable.
- » Verify that the cable has not been damaged.

## *Monitor/video*

Some common and easy problems to fix with monitors involve user errors: say, by adjusting the picture by using the knobs or buttons on the front of the monitor. There's nothing quite as annoying as going to a user's desk to look at a "broken" monitor only to find that the user has reduced the contrast and brightness to zero, leaving the image faint or nonexistent.

In addition to contrast and brightness, monitors usually offer horizontal and vertical size and position adjustments.

When monitor problems are not related to these settings, they might be related to power input or video cable problems (which are easy to correct). Because of the high-voltage capacitors and charges that are maintained by internal components, repairs of the internal components should be left to a good repair shop.

Users have many common monitor symptoms. Here are some of the most common:

- » **Incorrect colors** may be caused by front panel adjustments, or bent or damaged pins on the video cable connectors (which can be easily fixed), but more complicated issues would involve a trip to the repair shop or simply replacing the monitor.
- » **Burnt or damaged pixels** affect LCD and LED displays and are irreparable, so after the number is sufficient to affect the person using the monitor, the monitor should be replaced or rotated to a user who is more tolerant of the missing pixels. I have had users extremely bothered by one burnt pixel in the top-left corner of their screen, but other users with a dozen random burnt pixels on their screen hardly even notice the dots are missing. In some cases, the damaged pixel will be visible only when displaying one of the primary colors. While this problem can occur plasma displays, it is rare.
- » **Screen flicker** might be related to the internal power supply, but it is more often related to trying to run the monitor above specifications for color depth, resolution, and refresh frequency. Or, the refresh frequency is just set too low. These are OS-level settings, so they can easily be resolved in the Display control panel.
- » **Burn-in or image sticking** is caused when a single image is displayed one area of a screen for an extended period of time. Plasma screens can suffer from burn-in, while LCD and LED screens can have an image sticking. Image sticking is due to a charge buildup in pixels, and can be reversed.



Video problems can also be caused by your video card, which might not support settings to correctly communicate with your monitor and use appropriate resolution, color depth, and refresh settings for the monitor. If you have slow screen redraws, which can result in slow screen refresh or screen flicker, the video card might not have enough processing power or video RAM. If your computer has an integrated video card, you might be able to allocate more RAM to be used as video RAM. The final resolution for video card problems is getting your video card replaced.

If your system has a blank screen on boot-up, but the system does have a system beep, then you should look at the monitor itself. This problem could also be related to CMOS settings related to video card selection or BIOS configuration. These are all areas in which to examine for the source of the issue.



FOR THE  
EXAM

All video problems that are reported by a user will have to do with the video card or the monitor or both, and will likely have to do with trying to get more out of the system than it is capable of.

## *Serial ports*

Serial and parallel port problems can be caused by connectors, OS settings, and CMOS settings. Here are a few troubleshooting tips if you're having a problem with one of these ports:

- » **Check connectors for pin damage and check cables** for damage at the ends or along the cables themselves. Often cables running along the floor get run over by users' office chairs.
- » **Watch cable length.** Both serial and parallel specifications have maximum limits to the overall cable length, and exceeding these limits can cause intermittent communication problems with devices. Serial (RS-232) cables have a length limit of 50 feet (15 meters) when communicating at 19,200 bps, but that limit increases to 3,000 feet (914 meters) if you communicate at only 2,400 bps.

» **Serial ports** might be disabled in the Device Manager. Right-click My Computer, choose Properties, click the Device Manager button on the Hardware tab of the System Properties dialog box, and make sure the ports are enabled. If you are using Windows Vista, right-click Computer in the Start menu, choose Properties, and click the Device Manager link on the left pane of the System screen. There's nothing worse than spending a few hours trying to install a device to find out that the port you are connecting to was disabled.

In addition to being disabled at the OS level, the port may be disabled in the CMOS.

» **Verify the connection speed and data characteristics** for both serial ports and modems, and verify that they match with the device you are communicating with. These are specified by speed, data bits, parity, stop bits, and flow control.

- The *speed* is measured in *bps (bits per second)* and ranges from 110 bps to 115,200 bps.



TECHNICAL  
STUFF

Speed used to be measured as *baud rate* (after its creator Jean Maurice Emile Baudot), which is a modulation rate or state change. Baud used to match up with bps (bits per second). With current modulation, encoding, and compression techniques, the bps rate is substantially higher than the phone line's baud rate (2,400 baud). Many people incorrectly use the term *baud* when referring to bps.

- *Data bits* are either 7 bits or 8 bits.
- *Parity* may be set to odd or even and is used to verify the contents of a byte (8 bits) of data. Parity uses the eighth bit of a byte and sets the total value of the byte to either odd or even, depending on the parity setting.
- *Stop bits* are sent after the data to signify that the data byte has finished. Stop bits will be 1 or 2 bits long.

- *Flow control* manages the rate of data transfer between the devices, and it allows for transfer at higher rates. Without flow control, the sender can send data only at a rate that guarantees that the receiver can deal with, or process, the data that it is receiving. When using flow control, if the receiver is about to be overwhelmed or needs a pause to clear a backlog of processing, it can use the agreed system to signal a pause or to request more data.

## **USB**

Some common problems that you can encounter with USB include BIOS support, OS support, driver issues, version incompatibilities, and power requirements for devices. Here are some USB troubleshooting tips:

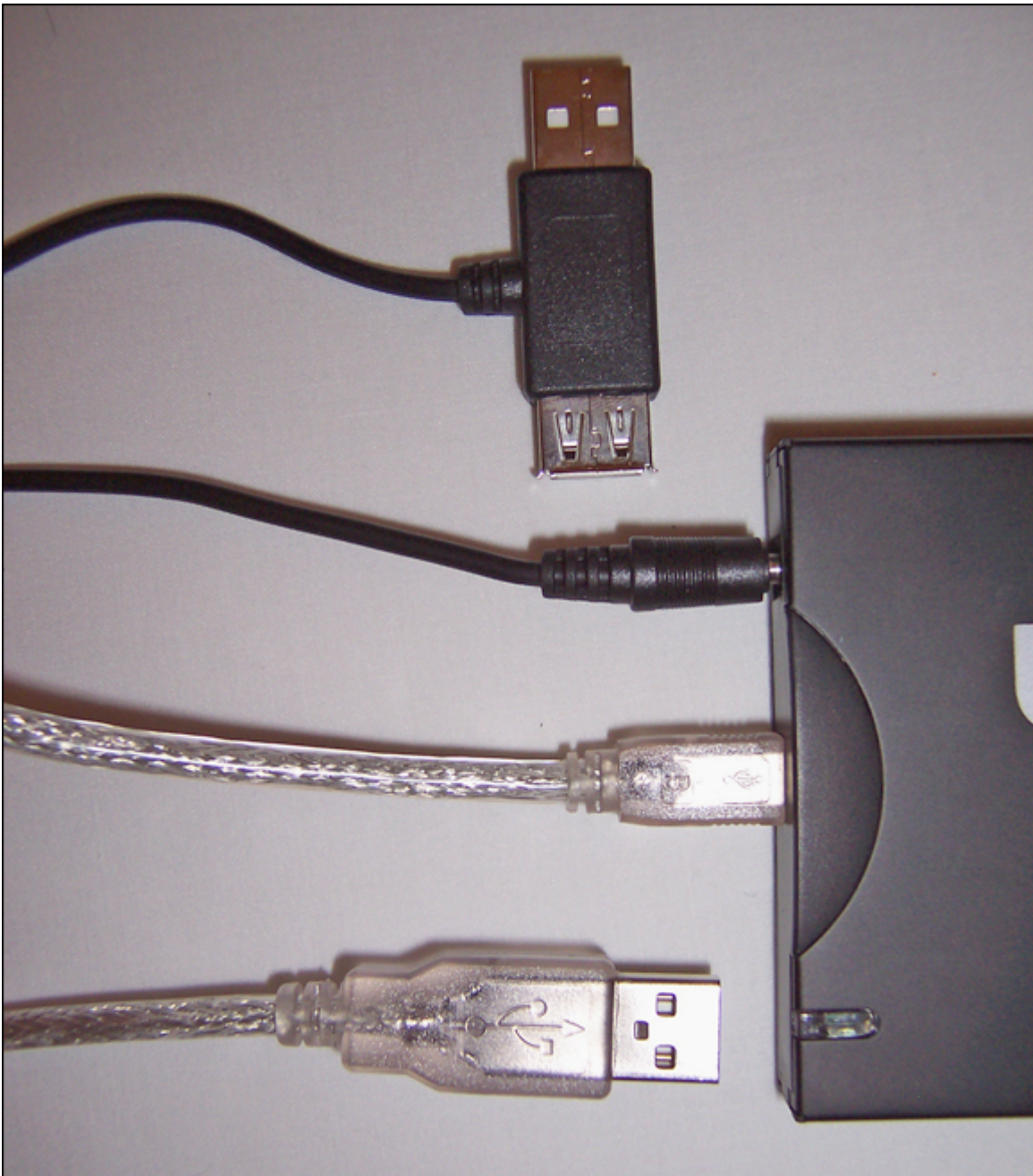
- » Like with all the peripherals that I cover, check all cables and connectors to ensure that they are properly connected and that the cables are not showing signs of damage or exceeding distance limitations for the technology.
- » Not all systems provide BIOS support or have adequate support for USB, so if you are encountering problems, check with the motherboard manufacturer for a firmware update that addresses your issue.
- » Just like serial and parallel ports, USB ports can be disabled in the CMOS or through the OS, and this should be checked if the ports don't seem to be working.
- » If the USB ports are enabled but are not working, the issue could be hardware related. You can look at doing a repair; or, in the case of a desktop computer, adding a separate USB controller via PCI or PCI Express.
- » If the devices are detected but are not functioning, you might want to ensure that correct drivers are available to the OS.
- » Although most devices are backward compatible, you might encounter performance or other errors when mixing USB 3.0, 2.0, and 1.x devices and controllers.



**REMEMBER** USB 3.0 or USB 2.0 devices plugged into USB 1.x ports will perform slower because of the restrictions of the USB 1.x specification. If devices are not performing at the expected level, check for this situation. Ensure that you match the type of device to the matching port to ensure that you get optimal performance from the device. Backward compatibility between these technologies will always result in slower performance if both the USB port and USB device do not match USB levels. For best performance, use the highest-level device in a matching USB port. For example, do not use a USB 3.0 device in a USB 2.0; make sure it is in a USB 3.0 port.

- » Finally, because most USB devices are powered from the bus, some devices may have power-related problems. Although the USB specification can provide up to 900mA of power to a single device through a Type-A connector, some USB controllers enforce the specification's low-power-mode startup at 100mA and then expect the device to request the necessary amount of power in 100mA increments.

If the device is dumb, such as a USB lamp, it does not have circuitry to communicate with the USB controller. Because it cannot communicate with the controller, it will take whatever power it can get, so it might not get the power that it requires to function properly. Other devices, like some USB hard drives, require up to 1A of power, and this can be supplied by special double-connector USB cables or cables to draw power from other USB ports. [Figure 2-4](#) shows the back of a USB hard drive, with a thick, silver USB cable and a thin, black power cable to be used for additional power. The connector on the end of the power cable is a *pass-through connector*, which would allow for another device to share the port that is being used to supply power to this drive. This sort of cable is required because some controllers will not allow devices to exceed the USB specified power per port.



**FIGURE 2-4:** Here is a device powered by two USB ports, using a pass-through connector for the second port.

All the troubleshooting techniques for USB devices can also be applied to FireWire devices.

## *Power Supplies and Batteries*

When troubleshooting power supplies, you first need to do the following two things:

- » **Country:** Make sure the power supply is configured for use in the country where the computer operates. Different countries have different standards when it comes to supplying power, and the computer's power source needs to match that.
- » **Flow:** Make sure the power supply is actually getting power. Checking this is easy enough — just see whether the fan is running.

In addition, ensure that all power supply connectors are correctly attached to devices, including the motherboard. You can test the power coming from the wall receptacle with

- » **An inexpensive receptacle tester:** Recommended
- » **A noncontact voltage indicator:** Recommended
- » **A multimeter:** Not recommended because of the risk involved at the voltage level being tested

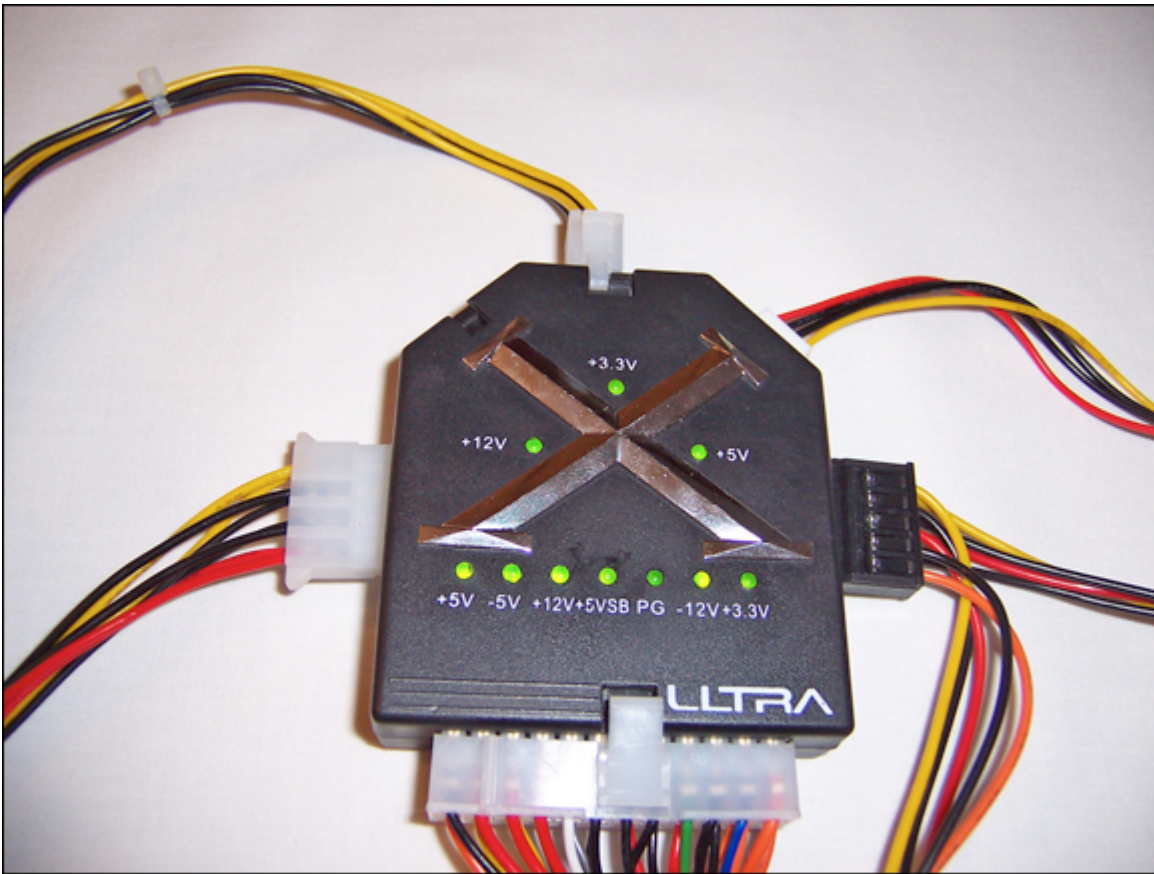


**REMEMBER** Power cords can be tested for continuity by using a continuity tester or a multimeter. To learn more about using a multimeter, refer to Book 8, [Chapter 1](#).

## *Testing power supplies*

Power supplies can be tested with inexpensive testers, as shown in [Figure 2-5](#). The tester will ensure that the power supply works and provides the proper voltages on each pin of the connectors. The tester in [Figure 2-5](#) supports 20/24 pin power, 12V, peripheral, floppy drive, and SATA connectors. If you suspect a problem with just one of the power connectors or one of the lines leading from the power supply, you can use a multimeter to test the connector, as described later in this section.





**FIGURE 2-5:** A power supply tester can save time when testing voltage supplied by power supplies.

In some cases, your power supply might be functioning correctly, but the problem might be that you are attempting to power too many devices, exceeding the total output of the power supply. Power supply testers cannot verify that your total draw does not exceed the amount supplied by the power supply; for that, you need to add up the power usage by hand. For information regarding the draw by devices, see Book 2, [Chapter 6](#). If you suspect that you are exceeding the power output of the power supply or the device bus, you can disconnect or unplug some of the devices and see whether the system returns to normal operation (with the exception of the missing devices).

I was recently troubleshooting a system with three out of five PCIe device slots occupied, and a Host Bus Adapter (HBA). We had sporadic failures on the HBA connecting to the SAN, and had the same issue on five identical servers. It turned out that one of the cards on the server was

drawing four times the power of a typical PCIe card; the HBA was the last card on the bus and was being starved for power. Upon removing the high-draw card, all other devices started working properly. Power issues can be tricky to locate and resolve. In this case, the problem was not the power supply, but rather the power limits of the PCIe bus.

## *Unexpected shutdowns, continuous reboots, and no power*

If the power supply is not functioning or does not have enough juice to power all the components of your system, replace it. Other issues that are often a result of defective power supplies include

- » Power-up or system startup failures or system lockups
- » Intermittent rebooting or lockups during normal operation
- » Intermittent memory errors
- » Intermittent device failures
- » Continual rebooting
- » Hard disk and fan simultaneously failing to run because of a shortage of current
- » Thermal failures and overheating because of fan failure
- » Electric shocks received when touching system case or connectors
- » System operations halted or rebooting from static discharges



**REMEMBER** When dealing with intermittent issues, such as shutdowns or failures related to heat, the device that is having the issue may become permanently damaged from overheating, and there may be cascading damage to other devices or data on storage media. Hard drives do not respond well to erratic power loss. These issues should be resolved as soon as possible, and while the data may still be safe and recoverable, a backup should be taken as soon as you



see symptoms. For example, if you note that a fan does not spin, you should immediately consider that the issue may not be with the fan at all, but rather with the power supply. If there is no fan spin and no power to other devices, then the issue is well beyond that of the fan and likely with the power supply.

Because ATX power supplies use a soft power switch, they need to be connected to a motherboard to be turned on. So, to test the main power connector — the one that connects to a motherboard — you need to

- » **Have the power-on pin shorted:** Not recommended
- » **Use a power supply tester:** Recommended and preferred; refer to [Figure 2-5](#)
- » **Back-probe the connector when the computer is running:** Not preferred, but acceptable; see [Figure 2-6](#)



**FIGURE 2-6:** Back-probing power connectors is a standard method for testing power in systems.

Most Molex-type power connectors can be *back-probed*, which is done by having your multimeter's black probe connected to ground and your

multimeter's red probe inserted into the back of the connector (which, in most situations, has sufficient space to allow the probe; see [Figure 2-6](#)). In this figure, the black probe is grounded, and the red probe is testing the 12V lead on the Molex peripheral connector. This result is valid because it is  $\pm 5$  percent, which is within the specification for power connectors. There is a minimal risk of damaging equipment if this procedure is done correctly, and it allows you to see on the live system what the power issues might be. Read Book 2, [Chapter 6](#) to see what the appropriate voltages are for each pin.



FOR THE  
EXAM

Power supply problems can result in problems with other systems. Check the question for keywords that suggest an issue with the power supply, in addition to the other device(s) mentioned.

## *Getting an A+*

In this chapter, you examine

- » Troubleshooting processes to follow when approaching a non-functional device
- » Sources of troubleshooting information, such as appearance, smell, and noise from a device
- » Troubleshooting major components, such as motherboards, drives, and peripherals
- » How each major component inside the computer system has unique troubleshooting steps

## *Prep Test*

- 1. You have been working on replacing hardware in a computer. When you are done, you power on the machine and hear a single short beep. What can you determine from this beep?**

- (A) There was a memory error detected during the POST.
  - (B) The POST completed successfully.
  - (C) You failed to reconnect the main power to the motherboard.
  - (D) An incorrect boot device is selected.
- 2. You have just installed a new application on your Mac OS X computer and when launching it, you are shown a rotating multicolor pinwheel in the center of the screen that does not go away. What tool can you use to help to diagnose this issue?**
- (A) Task Manager
  - (B) Event Viewer
  - (C) Activity Monitor
  - (D) `TSList.exe`
- 3. You have been examining a system and have been inspecting the power supply. Which issue doesn't indicate a possibly failing power supply?**
- (A) CPU thermal speed reduction
  - (B) Power-up failure
  - (C) System halt
  - (D) Internal devices receiving 12V and 5V
- 4. You are examining a system on your bench to ensure that all components are functional. What components can be tested by BIOS self-tests? (Select all that apply.)**
- (A) Hard drives
  - (B) CPU temperature deviations
  - (C) Magnetic media
  - (D) Memory
- 5. How does the system BIOS report major startup errors or configuration issues?**

- (A) Screen flashes
  - (B) Beep errors
  - (C) Error message dialog boxes
  - (D) Audio interruptions
- 6. You are looking into why a system has started to perform much slower than normal. This issue happened suddenly. What can be the cause of reduced CPU performance?**
- (A) Overuse of CPU cycles
  - (B) Addition of RAM
  - (C) Heat sink fan failure attributable to power supply failure
  - (D) Removal of the J7 motherboard jumper as defined by the ATX 1.2 standard

## Answers

1. **B.** A single short beep denotes that the POST process completed successfully. See “[\*POST errors.\*](#)”
2. **C.** On a Mac computer, the rotating pinwheel is the *spinning wait indicator*, which tells you there is something happening on the computer with an indeterminate completion time. If it hasn’t completed within an expected time limit, the Activity Monitor is the application to use to help determine if the issue is with the application or another application or process on your computer. Review “[\*Proprietary crash screens.\*](#)”
3. **D.** Power levels for internal devices are supposed to be 12V and 5V. Peruse “*Power Supplies and Batteries.*”
4. **A, D.** The system BIOS on some systems allows for testing of IRQs, memory, hard disks, CPU processing ability, and most internal components. Peek at “[\*CMOS, BIOS, and UEFI.\*](#)”
5. **B.** Beep errors are the standard way that major system startup failures are reported to the user. Look over “[\*POST errors.\*](#)”

6. C. Reduced CPU performance is often caused by the temperature of the CPU exceeding limits, and it reduces power to reduce the temperature. Excess temperatures usually occur when the heat sink fan fails. Study “[\*Processor/memory\*](#).”

# Book 5

# Operating System Basics

## Contents at a Glance

### Chapter 1: System Design and Operating Systems

[What Is an Operating System?](#)

[32-bit \(x86\) versus 64-bit \(x64\)](#)

[Looking at the Windows OS](#)

[Welcome to the Linux World](#)

[Understanding the Mac OS](#)

[Difference and Similarities between OSes](#)

[Choosing an Optimal System](#)

[Getting an A+](#)

[Prep Test](#)

[Answers](#)

### Chapter 2: Windows Operating System Functions

[Identifying Major Operating System Functions](#)

[Understanding Major Operating System Components](#)

[Navigating Your Computer](#)

[Using Tools and Configuration Utilities](#)

[Locating Major Files](#)

[Examining Windows Features](#)

[Virtualization Platforms](#)

[Virtual Desktops](#)

[Going to the Cloud](#)

[Virtual Applications](#)

[Getting an A+](#)

[Prep Test](#)

[Answers](#)

## **Chapter 3: Installing and Upgrading Windows**

[Understanding Installation Methods](#)

[Preparing for Installation](#)

[Performing Attended Installations of Windows](#)

[Performing Unattended Installations of Windows](#)

[Verifying and Troubleshooting the Installation](#)

[Upgrading Windows](#)

[Installing or Removing Additional Windows Components in Windows 10](#)

[Restoring User Data Files](#)

[Getting an A+](#)

[Prep Test](#)

[Answers](#)

## **Chapter 4: Managing Files and Directories**

[Identifying File-Naming Conventions](#)

[Understanding File Attributes](#)

[Getting an A+](#)

[Prep Test](#)

[Answers](#)

## **Chapter 5: Command Prompt Procedures**

[Using command.com and cmd.exe](#)

[Executing Your Privileges](#)

[Managing Directories](#)

[Copying and Moving Files](#)

[Performing Diagnostics and Tuning Performance](#)

[Getting Active with Group Policy](#)

[Working with Other Useful Commands](#)

[Getting an A+](#)

[Prep Test](#)

[Answers](#)

## **Chapter 6: Working with System Files and the Boot Process**

[The Power-On Self-Test \(POST\) Process](#)



[Standard Boot Process for Windows](#)

[Managing Memory and Virtual Memory](#)

[Getting an A+](#)

[Prep Test](#)

[Answers](#)

# Chapter 1

## System Design and Operating Systems

---

### IN THIS CHAPTER

- » Identifying the features, functions, and hardware requirements of the Windows OS, Linux OS, and Mac OS
  - » Working with Linux commands
- 

Although it seems like we live in a Windows world, other operating systems (OSes) live and thrive in the world. As a CompTIA A+ Certified Professional, you will encounter these OSes from time to time. You might even find that some OSes are more capable than Windows for specific jobs you need to do.

Of these other OSes, the ones you will see most are Linux and Mac OS. In this chapter, I briefly introduce you to these, as well as to Windows, and discuss their capabilities.

## *What Is an Operating System?*

All OSes are responsible for managing hardware, resources, and data. Each OS discussed in this chapter can perform these tasks with ease.

The responsibility of the OS regarding user interface (UI) consists of displaying an interface that always reacts the same way and makes it easy for users to perform tasks. A GUI (graphical user interface) attempts to make tasks easy and intuitive for the user. To provide a space for applications to run and for the user to manage his work, most OSes with a GUI use a “desktop” metaphor. That is, the desktop is a work area on which you have a computer, a place to store items, and a waste bin. All these elements also exist in the GUI.

The look and feel of the GUI, such as the look of the windows that are used, also applies to the applications that run on the OS. When applications use the same look and feel as the OS, and by having the OS provide common routines and dialog boxes for opening and saving files, there is a consistent appearance for the user, which usually reduces the time required to learn new applications.



**REMEMBER** Although hardware requirements vary and installation procedures are very different, after you get into using the features of the OS, all three OSes I talk about have similar usability features that allow a user to become capable in any other OS with but a short orientation period.

## *32-bit (x86) versus 64-bit (x64)*

Processors have changed from 16-bit to 32-bit, and now the move is on to 64-bit processors. With each change, the internal processing power of the processor greatly increases. To maximize this processing power, you require an OS that can work with data the same way that the processor can work with the data.

In addition to most current Linux distributions and macOS, all current versions of Windows support 32-bit and 64-bit processors, depending on the version of the OS installed. For example, if you install the 64-bit version of the OS, you need 64-bit device drivers and applications to achieve performance benefit.

64-bit processors access memory using 64-bit data paths, and as a result, they have a much higher memory limit. 32-bit processes have a 4GB memory limit, while 64-bit processors have a theoretical limit of 16EB (exabyte), even though computer systems are not using all 64-bit for memory access.

When using 64-processors and 64-bit operating systems, you will typically achieve higher performance when using 64-applications, and

data will be able to move at a faster speed. Technically 64-bit systems do not support 32-bit applications, but most operating systems provide this through a compatibility process. Windows provides 32-bit application compatibility through a process called Windows on Windows (WoW), which provides a 32-bit environment for 32-bit applications to operate. Windows does not support 16-bit applications on 64-bit OSes, but does support them on their 32-bit OSes. See Book 6, [Chapter 2](#) for more information on application support.

## *Looking at the Windows OS*

I start at the top of the OS hierarchy with the Windows OS. The look and feel of Windows today is very different from the look and feel of Windows 3.0 when I started using it in 1990. Windows 7 through to Windows 10 have streamlined the UI and added features, such as Wireless Zero Configuration and the Windows Store, to make it easier to use your computer.

### *Comparing versions of Windows*

MS-DOS was awkward and intimidating for many people to use, as they sat there looking at the command prompt slowly blinking at them. Windows was first developed as a shell, or UI, to go on top of MS-DOS, making MS-DOS easier to user. By the time Windows hit its third iteration, it was a very usable tool. This product — Windows 3.0 — went on to become Windows 95, 95 OSR2, 98, 98 SE, and Me. Windows Me represents the end of this product line, which has always been, because of architectural limitations, a shell on top of some level of MS-DOS.

The Windows that we now know and use owes its roots to a Microsoft/IBM venture that built upon the IBM OS/2 family to produce a new, secure server OS. But in the manner of many partnerships, this one fell apart, and both parties took the fruits of their labors and went home. Microsoft took this work and created Windows NT 3.x. NT and 3.1 were chosen to be compatible with the version number of the other Windows OS. The Windows NT OS was more stable than earlier versions of Windows because of its architecture (NT; New Technology) and more

secure because of its file system (NTFS; New Technology File System). In addition to creating the server OS, Microsoft created a desktop OS in the form of Windows NT 3.x Workstation, which had the same core as the Windows NT 3.x Server but also had many of the server components removed.

The drawback to the OS was that the architecture was totally different from that of the Windows 9x family. Because of this difference, many applications written for the Windows 9x family standards did not work with the Windows NT family. This limitation has slowly been overcome with each successive version of the OS, albeit sometimes at the cost of some of the stability features. This family went through Windows NT 4.0 to 2000 and then to XP. Windows XP was targeted not only to the existing users of the Windows NT family, but also to the users of the Windows 9x family; as such, Windows XP took large steps at backward compatibility with older applications. This focus on security, stability, compatibility, and usability of the Windows NT family continues with Windows 10, which is the latest addition to the family.



**FOR THE  
EXAM**

The recent Windows OSes — Windows 7, Windows 8.1, and Windows 10 — are based on Windows NT, and not Windows 3.0 or Windows 9x. For the A+ exams, you should focus on Windows 8.1 and Windows 10 OSes, as Windows 7 is nearing the end of its supported lifespan.

## ***Windows families***

Each of the current popular versions of Windows, which you will encounter in your job as an A+ Certified Professional, has several editions. Each of these editions has its own features which are supported. You will need to match up the needs of the user to the features in each edition.

### ***Windows 7***

Windows 7 supports the following editions:

- » **Windows 7 Starter:** Many devices do not require a full version of Windows to operate. With all the advanced features, a greater stress is put on the processor in your computer. To satisfy this need, Microsoft released the Starter edition, which made a home for itself on netbooks and other low-end computing environments. This edition has limited numbers of GUI features for the user to modify, including having the visual styles limited to Windows 7 Basic.
- » **Windows 7 Home Basic:** With a limited number of features, and a reduced set of Windows Aero features, this edition of Windows was aimed at price-conscious home users and emerging foreign markets.
- » **Windows 7 Home Premium:** The full-featured Home edition, again, not being able to join an AD domain, was Home Premium. This edition supported all the Home user features, including Windows Media Center features.
- » **Windows 7 Professional:** The Professional name was back for the general-purpose business edition of Windows. This edition has all the business-required features, such as Encrypting File System, Remote Desktop, and Windows XP Mode. In the business market, this edition does most of the work for most organizations.
- » **Windows 7 Enterprise:** The Enterprise edition adds support for BitLocker Drive Encryption and UNIX application support, in addition to a host of other features. This edition is not available through retail channels.
- » **Windows 7 Ultimate:** Containing all the Enterprise and Home Premium features, this is the most feature-complete edition of Windows 7 and is available to everyone through standard retail channels.

### *Windows 8 and Windows 8.1*

Windows 8.1 represents a marginal but important upgrade to Windows 8. With the advancement of many features, Windows 8.1 provides stability and user interface benefits over Windows 8. On the user interface front, improvements were made to the Start screen: The Start button was added back to the desktop, and new features such as higher resolution displays

and Miracast streaming were added. Other than these and other enhancements, Windows 8 and Windows 8.1 are typically considered the same operating system when compared with Windows 7. Windows 8 and Windows 8.1 support the following editions:

- » **Windows 8 (8.1):** This is sometimes referred to as Windows 8 Core, and represents the core Windows 8 OS. As with Windows 7 Starter and Windows 7 Home Basic, many users do not require a version of Windows with all the bells and whistles. To simplify the offers of Windows 8, Microsoft reduced these offers to a single product. Unlike the Windows 7 versions, Windows 8 has all the main features users are looking for except for the Media Center and Corporate features.
- » **Windows 8 (8.1) Professional:** The Professional name is back again for the general-purpose business edition of Windows. Think of this version as being akin to Windows 7 Professional and Windows 7 Ultimate. This edition has all the business-required features, such as Encrypting File System, Remote Desktop, Virtual Hard Disk (VHD) booting, and BitLocker disk encryption. Media Center features are available as an optional download. In the business market, this edition does most of the work for most organizations.
- » **Windows 8 (8.1) Enterprise:** This edition has all the features of Windows 8 Professional, but is aimed at larger companies that chose to have access to Windows through the Software Assurance program. This version is not available through retail channels.
- » **Windows 8 (8.1) RT:** This version of Windows 8 is designed to run on the ARM processor, which was used in the first two generations of the Microsoft Surface tablet. Because the hardware was targeted to businesses, Windows 8 RT includes Microsoft Office 2013 and Microsoft OneNote, and support for joining Microsoft AD domains.

## *Windows 10*

Windows 10 represents the culmination of the Windows desktop OS. It continues to support many of the features you have come to know and trust from Windows, as well as many other features and enhancements.

Windows 10 is supported on many hardware platforms from computers, to

tablets, to phones, to Xbox, to HoloLens, to Surface Hub, to a variety of wearable devices.

One of the biggest changes with Windows 10 is its Windows as a Service (WaaS) model. WaaS is a perpetual upgrade model for Windows, which releases two upgrades per year with a mandatory upgrade requirement for users to remain in support. With the two releases put out every year, some organizations will be updating every six months, and the maximum amount of time that corporate editions may wait between upgrades is 18 or 30 months, depending on the release.

Windows 10 supports the following editions:

- » **Windows 10 Home:** This version of Windows 10 supports the core features of Windows 10, such as Microsoft Edge, Cortana, Windows Hello, biometric logon options, touch support, and universal apps through the Microsoft Store. What is missing from this version are features that are considered to be corporate features. Windows 10 Home, as the name suggests, is designed to meet the needs of the typical home user.
- » **Windows 10 Pro:** The Professional name is back again for the general-purpose business edition of Windows. Think of this version as being akin to Windows 8 Professional. This edition has all the business-required features, such as AD support and domain access, Encrypting File System, Remote Desktop, Virtual Hard Disk (VHD) booting, BitLocker disk encryption, BranchCache, and support to control the update process and make use of Windows Update for Business. In the business market, this edition does most of the work for most organizations. This version of Windows 10 bridges the gap between corporate and personal needs.
- » **Windows 10 Enterprise:** As with other versions of Windows 10, this edition has all the features of Windows 10 Pro, but is aimed at larger companies that chose to have access to Windows through the Software Assurance program (which is a perpetual licensing and support model for software). This version is not available through retail channels.



- » **Windows 10 Enterprise LTSC:** LTSC is the Long-Term Servicing Channel. Some organizations have computers performing control functions, such as security systems, kiosks, or production-line controllers. These systems do not need to support all of the Windows 10 features, such as modern applications, and the users of these systems do not want to be forced to upgrade three times a year as with the other Windows versions. The solution is Windows 10 LTSC. LTSC has a support lifespan of five years, but in providing this to users, many of the user-friendly features, such as all Microsoft Store apps, have been removed. Systems running this OS are expected not to be used by people for day-to-day computing, but rather they fill the niche for these background control systems.
- » **Windows 10 Education:** This edition has all the features of Windows 10 Enterprise, but is aimed at schools and educators with tailored features to make using Windows 10 in those environments easier. This version is also only available through the Software Assurance program, and is not available through retail channels.
- » **Windows 10 IoT:** With the wide adoption of small, single-purpose computers now found in a variety of devices, such as televisions, refrigerators, cars, and home security systems, Microsoft has released a Windows 10 Internet of Things (IoT) version. This version of Windows 10 is extremely lightweight and is designed to be used on these small-footprint, single-purpose computers.

### *Typical system requirements*

Although Windows started out with its roots in MS-DOS, current versions of Windows are based on Windows NT. For the most part, you will work with systems running on Windows 7, Windows 8.1, or Windows 10.

[Table 1-1](#) lists the system requirements for each version of Windows that you will likely encounter.

## **TABLE 1-1 System Requirements for Microsoft Windows**

---

---

	<b>Windows 7</b>	<b>Windows 8 (8.1)</b>	<b>Windows 10</b>
<b>Processor</b>	1 GHz or higher 32-bit or 64-bit processor	1 GHz or higher 32-bit or 64-bit processor	1 GHz or higher 32-bit or 64-bit processor
<b>Memory</b>	1GB RAM (32-bit) or 2GB RAM (64-bit)	1GB RAM (32-bit) or 2GB RAM (64-bit)	1GB RAM (32-bit) or 2GB RAM (64-bit)
<b>Hard disk</b>	16GB (32-bit) or 20GB (64-bit) available disk space	16GB (32-bit) or 20GB (64-bit) available disk space	16GB (32-bit) or 32GB (64-bit) available disk space
<b>CPU support</b>	Single or dual CPU	Single or dual CPU	Single or dual CPU
<b>Display</b>	DirectX 9.0 with WDDM 1.0 or better driver	DirectX 9.0 with WDDM 1.0 or better driver	DirectX 9.0 with WDDM 1.0 or better driver



**FOR THE  
EXAM**

Expect to get a question related to the hardware requirements for these Windows OSes.

Windows 8.1 has one extra requirement which Microsoft displays in the small print, and that is to access the Windows Store and to download and run snap apps, you require a screen resolution of at least 1024 x 768.

The biggest differences between the different Windows OSes are hardware requirements and some advancements in application compatibility. If you have a computer that is lower than or just meets the hardware requirements of an OS, you might want to consider using an older OS for that particular computer.

For instance, although a computer with 1GB of RAM and a 1-GHz processor meets the requirements for Windows 8.1, you might compare that with the base model of a car, without all possible options. For any OS, if you choose hardware at the minimum level, you will get minimum performance. Using hardware above that level is like buying an options package for your car. With 1GB of RAM and a 1-GHz processor, you will likely find that Windows 7 will offer somewhat better performance than Windows 8.1 or Windows 10 because it has less convenience and less

overhead. However, in this case, your cost would be losing Windows 8.1 and Windows 10 features.

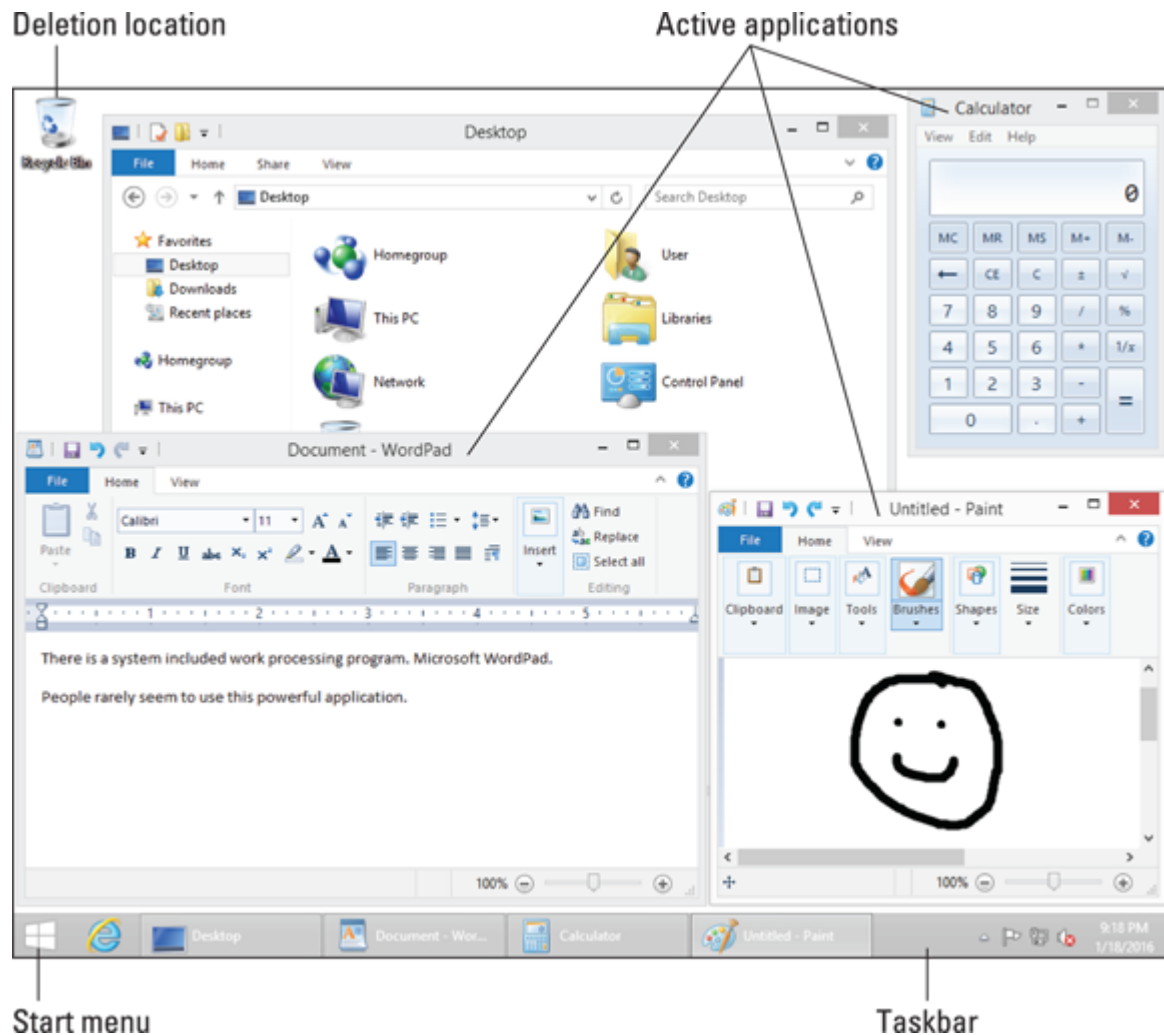
As you move backward in the Windows NT family (the base OS that the current Windows versions are based on), each version of the OS was designed to work with a lower level of resources. It then becomes a trade-off of features versus speed. There is a minimum level of the OS that you will be able to work with because of minimum requirements, such as security or USB compatibility.



**REMEMBER** You are the only person who can determine which OS is right for you, and that decision depends on what features you actually feel are important and the hardware that you have available. You are also the person to determine your minimum requirements, whether it is a computer with 1GB of RAM and 1 GHz processor or one with 16GB of RAM and a 4 core 3 GHz processor. What is good for one person may not be good for someone else.

## *Identifying GUI elements*

The Windows GUI follows the desktop metaphor I describe earlier, with your files, active applications, and a virtual trash can all within easy reach onscreen. A taskbar at the bottom of the screen allows you to quickly switch between open applications; it also holds a Start menu, from which you can quickly launch applications. See the Windows 8.1 GUI in [Figure 1-1](#).



**FIGURE 1-1:** The Windows 8.1 GUI.

The Windows interface introduced with Windows 95 “borrowed” (ahem) the features that were working in the other major graphical OS of the time (the macOS). Although there have been some functional and cosmetic changes to the GUI, there have not been any major changes to how the GUI functions or operates.

### *Special Windows 7 features*

Windows 7 supports seven main user interface features:

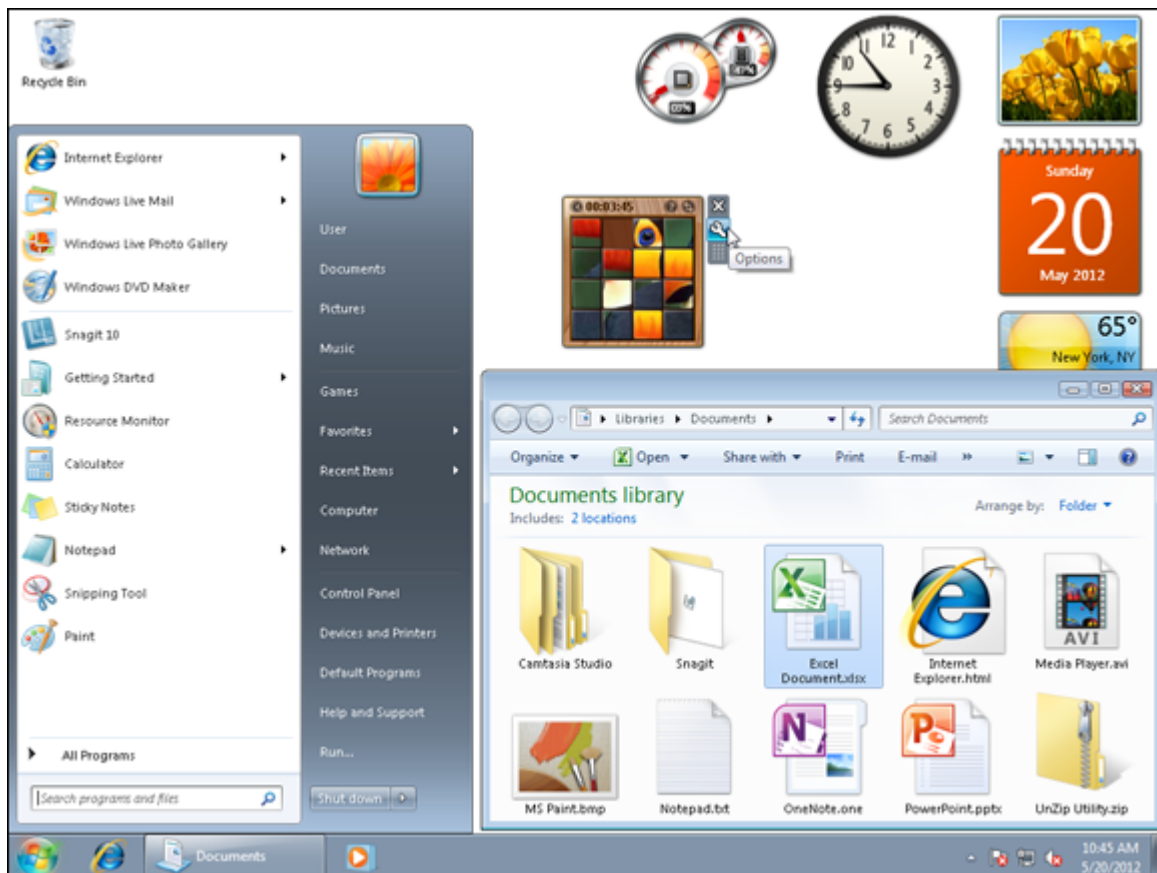
- » **User Access Control (UAC):** UAC adds a layer of authentication or security to the execution of tasks that could damage the OS. In Windows XP, a user needs to be given Administrator rights for certain

tasks. Windows 7, though, allows a user with less privilege to run most tasks, and asks for permissions prior to executing critical tasks.

- » **Gadgets:** Unlike the Sidebar interface from Windows Vista, gadgets are now no longer limited to the Sidebar area, but rather can be placed anywhere on the desktop. These can be seen in [Figure 1-2](#).
- » **Libraries:** Libraries combine files in various locations into what appears to be a single location. Documents is an example of a library, which can combine your personal files from multiple drives, so to you it appears that they are in a single location.
- » **Virtual Hard Disk (VHD) Support:** Support for mounting and reading data from Microsoft Virtual PC and HyperV virtual disk files. OS support for this disk format is so high that a Windows 7 installation can even be booted from a VHD file.
- » **XP Mode:** To improve compatibility with older applications, XP Mode allows you to run applications in an integrated Virtual PC installation, but your applications will look like they are running on Windows 7. This feature is designed to be a stop-gap in Windows XP to Windows 7 migration, allowing systems to be upgraded even though they have one or two applications that still require Windows XP. The goal is to provide the organization some additional time to get the software updated to allow it to run under Windows 7. Because this was a temporary measure, XP mode is removed in Windows 8.1, as companies should have had enough time to migrate those few problem applications.
- » **ReadyBoost:** Big reasons for performance issues on disks are the rotation of drives and the movement of disk heads. To reduce the effect of these delays, Windows 7 allows you to use flash memory (in the form of USB flash drives, SD cards, or CompactFlash) as a system cache for the standard hard drives in your computer.
- » **Action Center:** In Windows 7 and later OSes, the Security Center has been replaced with the Action Center. The Action Center will place a Flag in your System Tray to let you know you should look at something important. Like the Security Center, important items include

security topics, such as antivirus and malware warnings, and maintenance topics, such as backup and driver warnings.

- » **Pinning:** In addition to pinning shortcuts to the Start menu, Windows 7 and later OSes also allow you to pin applications to the Taskbar. If you locate an application in the Start menu, you can right-click on it to pin it to the Taskbar. You are also able to right-click on any running application in the Taskbar to pin it to the Taskbar.



**FIGURE 1-2:** The Windows 7 desktop.



**WARNING** The Windows Vista Sidebar and Windows 7 Gadgets, which made use of a common interface, have been found to contain security flaws. Because of this, these features have been removed in newer Windows OSes.

## *Special features of Windows 8.1*

Windows 8.1 provides several new enhancements over the previous version of Windows. Following are the features that appeared with Windows 8.1:

- » **Side-by-Side Apps:** You can maximize an application window if you drag toward the top of the screen, and if you drag to the left or right side of the screen, the window will resize to fill the left or right half the screen. This makes it easy to arrange two windows side by side for working in both windows.
- » **Start Screen:** Microsoft removed the familiar Start menu with the release of Windows 8 and replaced it with the Start screen. The Start screen provides access to pinned applications and further access to all the applications that would normally be visible in the Start menu. Using the Start screen and pinning of applications means that most applications you need will be right on the Start screen. [Figure 1-3](#) shows the Start screen from Windows 8.1.
- » **Metro UI:** Microsoft has been driving to consolidate its mobile and desktop interfaces. As an effort to do that, the default launch interface for Windows 8.1 devices (phones, tablets, and computers) is the Metro User Interface (UI), which is also called the Start screen rather than the desktop. As discussed in the previous bullet, the Start screen is a tile-based screen that launches desktop apps or Metro apps. Metro apps are full-screen apps that hide the desktop interface. In Windows 8.1, Microsoft returned the default interface to the desktop for computers, and users still accessed the Start screen by clicking the Start button. Windows 10 has continued with the same desktop styles as Windows 8.1, with an enhanced Start Menu and the same user interface to pinning and working with applications, as shown in [Figure 1-4](#).
- » **Multimonitor taskbars:** With the popularity of multiple monitors there has been one item missing: the Taskbar. The Taskbar only showed up on your primary monitor, until now. To see the Taskbar settings, right-click in a blank area of the Taskbar and select Properties. If you have multiple monitors, you will see an addition

section the Taskbar tab of the Taskbar properties. This will allow you to choose on which Taskbar you will see application icons. Your choices are

- All taskbars
- Main Taskbar and Taskbar where window is open
- Taskbar where window is open

» **OneDrive:** Cloud-based storage has become a hot topic, and Microsoft has integrated its cloud storage solution (OneDrive) directly into the Windows Explorer interface so working with files on OneDrive is no different than working with local files. Formerly named SkyDrive, OneDrive offers the extra bonus of having a web-based interface to access your files if you are away from your computer.

» **Windows Live Sign-In:** To go along with the OneDrive service, Microsoft integrates authentication for all its online services, including Mail, OneDrive, Xbox, and so on, through a Microsoft Account logon. Prior to adopting the name Microsoft Account, Microsoft called the account Windows Live. The Windows Live Sign-In is the common integration that provides access to all the Microsoft services.

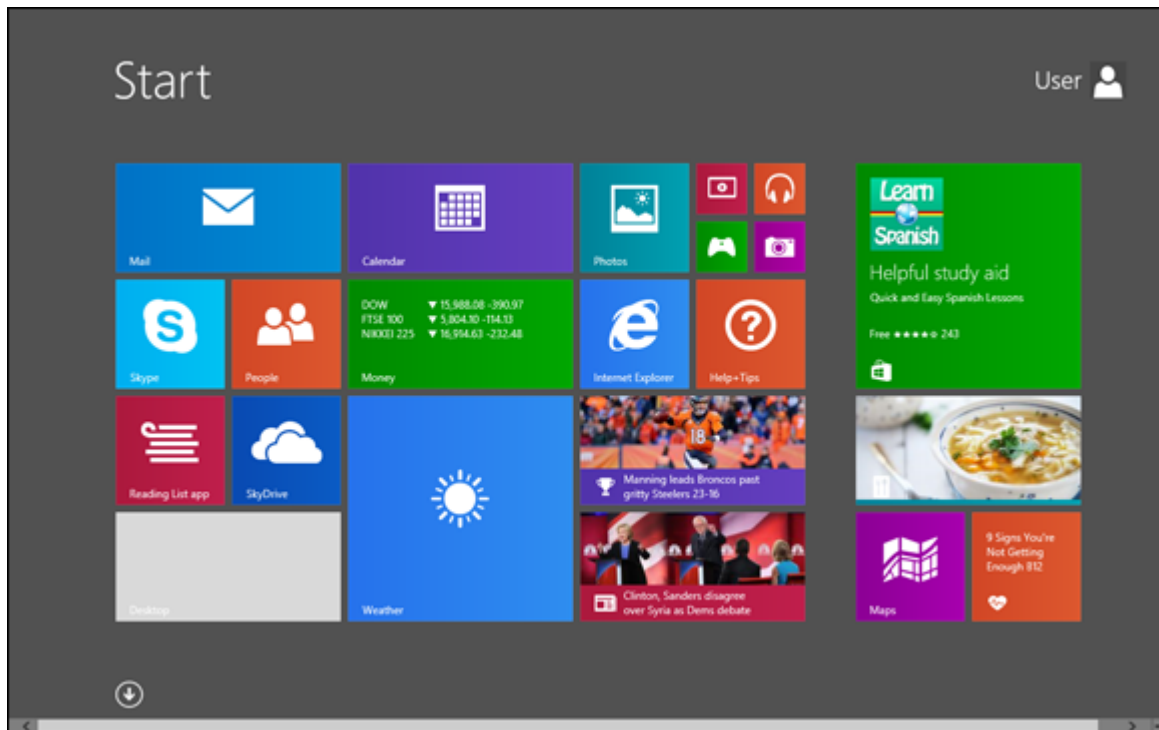
» **Windows Store:** Application developers are able to publish Windows 8.1 and Windows 10 applications to the Windows Store, making it easy for users to install a variety of free and purchased applications.

» **Charms:** Really designed for tablets and full-screen Metro apps, the Charms interface is reached by touching or dragging the mouse to the top-right or bottom-right corners of the screen. The Charms section of the screen provides the Search, Share, Start, Devices, and Settings buttons to access many common features on your device.

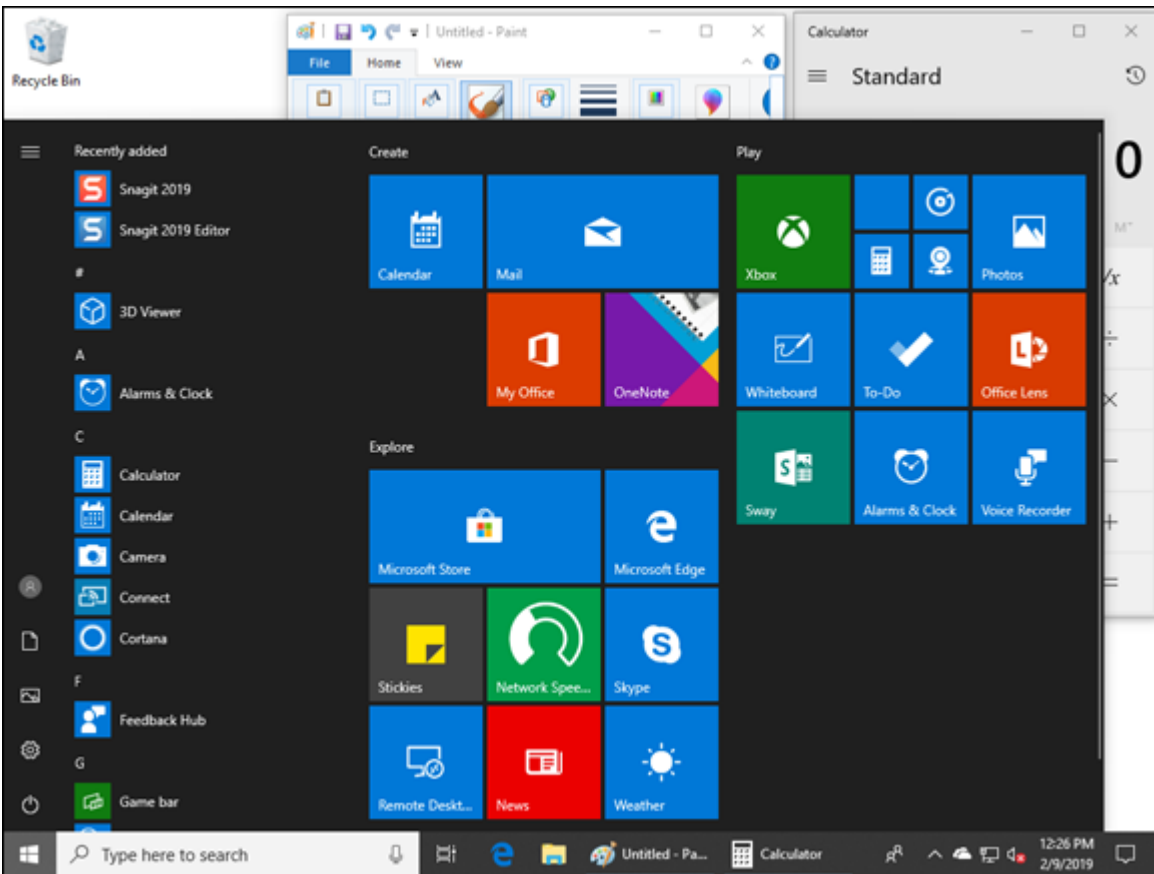
» **Windows PowerShell:** Scripting languages built into the OS have always offered advantages to languages that had to be installed. The primary advantage of built-in languages is that they are available when you need them. Shell scripting through batch files are as old as



DOS, and VBScript showed up in Windows with Windows 9x. PowerShell is the newest and most powerful scripting language to be included in the Windows OS and arrived with Windows 7. Microsoft relies on the Windows PowerShell scripting language for all new administration for servers and server applications, so you can expect it to be around for a long time.



**FIGURE 1-3:** The Windows 8.1 desktop.



**FIGURE 1-4:** The Windows 10 desktop.

### *Special features of Windows 10*

Windows 10 provides several new enhancements over the previous versions of Windows. Following are the features that appeared with Windows 10:

- » **Start Menu:** The Start menu is back. There is still support for full-screen menu on touchscreen systems, but for most part, the Start menu is the main interface to manage, launch, and control applications.
- » **Cortana:** Microsoft's digital assistant has come to the desktop. Cortana is integrated with search, but is not limited to search alone. It can remind you of important meetings and notify you to start heading to offsite meetings based on the current traffic on your route.
- » **Edge Browser:** Internet Explorer has been around for a long time, and Edge represents the new generation of web browsers on Windows 10.

- » **Multiple Desktops:** Instead of having all your open applications on one screen, you are able create multiple virtual desktops and organize your applications between them. This allows for a cleaner interface for your applications.
- » **Universal Apps:** Modern Windows apps are supported on any platform capable of running Windows, so if you are on a phone, tablet, desktop, or other device, you should be able to run the application and have a similar experience, without needing to deal with multiple versions of the application.

## *Welcome to the Linux World*

The UNIX OS was originally designed to control telephone switches for the Bell telephone network. It was designed to be highly stable and configurable. As it grew to maturity, it became popular for its stability and processing power. Over the years, UNIX went from solely a command line environment to having a GUI. Its popularity led to a young university student's creation, during the early 1990s, of a UNIX-like shell that would work on Intel-based systems. This student was Linus Torvalds, and he created Linus' UNIX, or *Linux*.

### *Comparing Linux versions*

Since the creation of Linux, it has been a worldwide group project, with Linus Torvalds controlling what components go into the Linux *kernel*, or the core components that make up the brains of the Linux OS. Many individuals and groups have contributed programming code to the Linux kernel, usually as completed drivers for hardware. The only thing that is common to all versions of Linux is the OS kernel. Beyond the kernel, there are applications that are used with the kernel to give you a system that you can actually use to accomplish tasks. You can literally download the kernel source from <http://kernel.org>, compile the applications that you want to use, put them together, and have a Linux system. Because it is that easy to make your own Linux system, there are currently just about as many Linux systems as there are tasks you want to accomplish with them.

When a group or company takes the Linux kernel, combines it with a UI (shell), and then bundles in a variety of applications, a *distribution* is created. All Linux distributions are cousins and have been created with the same core components. Where distributions differ are in the mix of tools that are bundled in the distribution, and any customization the creator of the distribution decides to include.

There are a few major distributions of Linux, which have changed over the years. The current major distributions include

- » Ubuntu
- » Debian — GNU/Linux
- » Fedora Core — Red Hat
- » Arch Linux
- » Knoppix
- » Slackware
- » SUSE — openSUSE
- » Linux Mint

The main difference among these distributions is packaging. They all run the same kernel (or core), and most applications they run are the same as well because the applications are written to the kernel specifications. The real difference is the wrapping material that ties these elements together. In most cases, this wrapping includes an OS installation tool and a packaging tool, which are used to prepare applications for installation and removal.

All distributions have a command line interface, and most also include a variety of GUIs. Common Linux-based GUIs include XWindows with several Window Managers, such as AfterStep, Black Box, Enlightenment, IceWM, and Window Maker, to name a few. In addition to these standard Window Managers, GNOME and KDE are two complete desktop interfaces that are popular. Ubuntu uses GNOME as its default desktop manager, but has added on its Unity shell to improve usability.

Most distributions have packaging tools based on one of two standards — Red Hat Package Manager (RPM) or Advanced Packaging Tool (APT) — both of which offer the ability to install dependent packages and resolve applications that conflict with each other. Both tools can also be configured to work with one or many networks or Internet package sources.

Applications written to Linux standards don't work on Windows-based systems but might work in the macOS environment. Some developers write Linux applications to common standards, such as Java or GTK+, which both have components that can be installed on Windows systems.

Each Linux distribution has its own set of revision numbers to identify the distribution version. What matters more than the revision number is the version of the kernel that is used, as well as revision levels on the shared libraries, which are common routines that are used by many applications. Typically, when you install a new application, it has specific requirements for revisions of both the kernel and shared libraries but does not usually care about the distribution revision level.



TECHNICAL  
STUFF

In addition to the Linux distributions I mention earlier, BSD UNIX is making several new inroads into the market. BSD started in the 1970s and has spawned many child distributions, such as FreeBSD, OpenBSD, and PC-BSD.

### *Typical system requirements*

Different Linux distributions have different system requirements. To take a distribution at random, openSUSE Linux requires the following:

- » 1.6 GHz modern processor or better
- » 1GB of RAM or better
- » 3GB of hard drive space for a minimal install
- » 800 x 600 display

Most distributions have similar installation requirements and can install on substantially less hardware, depending on the purpose of the installation. For instance, some Linux distributions are designed to run routers and firewalls, and these single-purpose distributions require substantially less hardware to function.

Linux runs on all the same hardware on which Windows runs, as well as several hardware platforms on which Windows does not run. If you would like to test Linux, you can find several Live CDs that allow you to boot the distribution directly from the CD without installing any files on your hard drive. These Live CD versions can be downloaded from the distribution's web page, but you will find helpful information to help you choose a distribution from either [www.linux.org](http://www.linux.org) or [distrowatch.com](http://distrowatch.com).



**TIP**

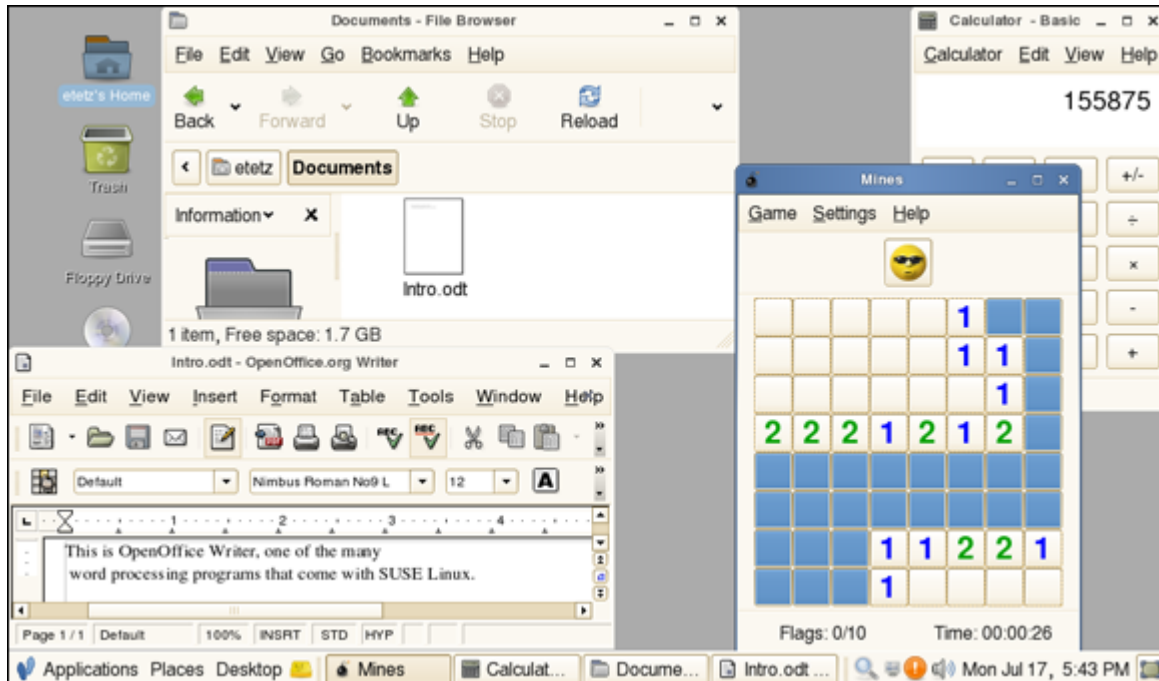
If you really want to get started with Linux, a great place to begin is *Linux Bible*, 9th Edition, by Christopher Negus (published by John Wiley & Sons, Inc.). It covers the major Linux distributions.

A wide variety of file systems are supported by Linux; some are journal based (such as ext3 and reiser) and others are not (such as ext2). *Journal-based file systems* keep track of writes to the file system, and thereby provide better and faster recoverability in the event of a system crash or power loss. Most Linux distributions will install onto one of these file systems. Like with Windows NT-based systems that support NTFS-based security, most Linux-based file systems support per user or per group security on files and folders.

## ***Identifying GUI elements***

Although many people use command line systems exclusively when using Linux, many GUIs can be used as well. The GUI loads as a separate element on top of the core command line OS. Even when you are using a GUI, you will likely find occasions when you need to go back to the command line or a command line window (a *terminal window*) to accomplish your tasks. [Figure 1-5](#) shows the GNOME desktop environment, which is one of the popular GUI environments for Linux.

KDE is the other major desktop environment; and then there are several other Window Managers that may be used, such as Window Maker, IceWM, and FVWM with XP Theme (which looks like Windows XP), each giving you a different interface for window management on your Linux system.



**FIGURE 1-5:** The GNOME desktop environment in action.

All GUI environments available for Linux have the same basic features for window management and work in conjunction with a file management application. The major differences between these systems are in the implementation and extra features, such as auto-mounting CDs as they are inserted into the drive. You should note that the GNOME desktop features and layout are similar to those used by Windows XP.

## *Getting around the Linux Terminal*

Underneath the desktop management interface of your Linux system is the powerful core of the Linux OS. The core interface of Linux is a command-line interface, which, if you have installed a graphical desktop, you will access through a terminal interface. The default terminal interface application is ingeniously named Terminal, Terminal Emulator, or xterm. You can usually get to the terminal program by opening your application

menu and locating Terminal in Accessories, but this varies based on the desktop interface you have installed for your Linux computer. If you do not have a desktop interface, you will automatically be at a terminal screen.



TECHNICAL  
STUFF

As you find out later in this chapter, the Apple's macOS is based on a FreeBSD kernel, which allows you to run most of the commands listed here when using Terminal.

There are a few major differences between Windows command line tools, which are covered more deeply in chapter Book 5, [Chapter 5](#):

- » Command and options (or switches) are all case sensitive.
- » Switches are prefaced with one hyphen (–) or two hyphens (—) if the full name of an option is used, rather than a forward slash (/).
- » Help for a command is accessed by the switch –h or —help rather than /h.
- » Multiple switches can be used with a single hyphen: for example, ls –al to list all files using a long directory listing.

In addition, wildcards can be used with these commands:

- » \* : An asterisk represents 0 or more characters.
- » ? : A question mark represents 1 character.
- » [ ] : Square brackets allow for a single character which is found inside of the brackets.

Following is a discussion of the common Linux commands you should be familiar with.

### *man*

The easiest way to get help for almost any Linux command is to use the Manual Page or man page. The `man` command is used to access the man



pages. To use the `man` command, simply type **man** followed by the command for which you need help. Here is an example of getting help with the `ls` command:

```
man ls
```

You quit the `man` command by typing **q**.

## *ls*

`ls` is the list files command, which is similar to the `dir` or directory command in Windows. Common options for the `ls` command include (each starting with a hyphen):

- » **a**: Display all files
- » **l**: Use long format, displaying file information
- » **R**: Recurse or list contents from sub-directories as well as the current directory

## *cd*

The `cd` command is short for *change directory* and is used to change the present working directory to something else. This command can take a relative name or a fully qualified name. Relative path names start with a directory name, while fully qualified path names start with a `/` for the root of the file system.

To navigate directories using relative names, use the following options (starting with a hyphen):

- » **.**: A directory path starting with a single period refers to a path starting with the current directory.
- » **..**: Two periods used a directory anywhere along a path refers to the parent directory. To move to the parent directory, use the following command:

```
cd ..
```

## *mv*

The move (`mv`) command is used to move files or directories from one directory to another. A move command does not actually touch the file, but rather it modifies the file directory entry for the file. To move files, specify a source directory or file and a target directory. Common options for the `mv` command include (starting with a hyphen)

- » **f:** Force will overwrite any files in the target directory.
- » **i:** Interactive requires a prompt before overwriting any files.
- » **n:** No clobber will not overwrite existing files.
- » **u:** Update will only copy files when the source file is newer or the target file does not exist.

### *cp*

Similar in syntax to the move command, the copy (`cp`) command creates a copy of files or directories in a new or target location. Common options for the `cp` command include (starting with a hyphen)

- » **f:** Force will overwrite any files in the target directory.
- » **i:** Interactive requires a prompt before overwriting any files.
- » **n:** No clobber will not overwrite existing files.
- » **u:** Update will only copy files when the source file is newer or the target file does not exist.
- » **r:** Recursive mode recursively scans directories and copies any sub-directories.

### *rm*

Remove is the name of the `rm` command. It is used to remove files. To remove empty directories, the `rmdir` command is used. You will want to use extreme care when using wildcards with the remove command, as you can do serious damage to your computer if you remove files that are needed by the operating system. Common options for the `rm` command include (starting with a hyphen)

- » **f:** Removes files without prompting for confirmation

» **r**: Recursively scans directories and removes any files and directories

## *chmod*

The `chmod` command is used to change file or directory access permissions. Using the `ls -l` command enables you to see current permissions. The permissions displayed in the permissions block (rwxrwxrwx) are for the User or Owner, Group, and Others (ugo). The permissions can be read, write, and execute, and are assigned numeric values of 4, 2, and 1, respectively, which are added together form the permissions level.

```
etetz@linuxvm:~/Documents$ ls -l
total 12
-rwxrwxrwx 1 etetz etetz 669 Jan 4 21:07 MyFirstFile.txt
-rw-r-xr-- 1 etetz etetz 669 Jan 4 21:07 MySecondFile.txt
-rw-r--r-- 1 etetz etetz 669 Jan 4 21:07 MyThirdFile.txt
```

You can use the `chmod` command with permission names or with numeric permission levels. You should be familiar with both. For example, to use permission names to add the write and execute permissions for Group to a file called `MyThirdFile.txt`, the command would be:

```
chmod g+wx MyThirdFile.txt
```

In addition to `+` to add permissions, you may use `-` to remove permission or `=` to set them to a specific value. In addition to granting permissions to User, Group, and Other, you may grant permissions to All.

To use numeric permissions to set permissions to a specific level, the command is similar to the following command, which grants the User full permissions (read, write, execute), the Group read and write permissions, and Others read permissions. To give the user full permissions, total the individual permission of read (4), write (2), and execute (1), which totals 7, then total the group permission of read (4) and execute (1), which totals 5. The command would be:

```
chmod 754 MyThirdFile.txt
```

Common options for the `chmod` command include (starting with a hyphen)

- » **v:** Verbose mode displays diagnostic information for every file processed.
- » **R:** Recursive mode recursively scans all sub-directories for files matching a certain pattern.

## *chown*

The `chown` command is used to change the ownership of a file. It enables you to set an owner user and an owner group, which were discussed in the previous bullet on the `chmod` command. If you refer back to the directory listing displayed in the `chmod` command, you will see `etetz` listed twice on each line. The first is the owner and the second is the group. With the creation of each user account there will also be a matching group by default. An example of the command would look like the following, which sets the owning user to `bsmith` and the group to `audiusers`:

```
chown bsmith:audiusers MyThirdFile.txt
```

Common options for the `chown` command include (starting with a hyphen)

- » **v:** Verbose mode displays diagnostic information for every file processed.
- » **R:** Recursive mode recursively scans all sub-directories for files matching a certain pattern.

## *locate*

The `locate` command makes use of the database of file system names. If you have recently installed the `locate` command or if you have recently added or removed many files from your computer, you will want to use the `updatedb` command to update the database of filenames.

You can use the `find` command or a combination of `ls` and `grep` to get a listing of files on your computer, but these commands require a scan of the file system, which can be slow. The `locate` command scans the database rather than the file system, which is substantially faster when trying to locate files on your computer. The output of the `locate` command can still be redirected into `grep` for further filtering.

For example, to find all files that contain `pwd` in the path, use the following command:

```
locate pwd
```

## *grep*

The `grep` command is used to find strings of data. It can be given a filename to look in for the string of text, or it can take the data through the pipe command.



TECHNICAL  
STUFF

The pipe ( `|` ) command is used to direct output from one command into another command. An example of this is to filter directory lists from the `ls` command using `grep`. Here you are shown a list of files in the `/bin` directory that start with the letter `p` and contain the string `wd` somewhere in the filename or path:

```
ls /bin/p* | grep wd
```

Common options for the `grep` command include (starting with a hyphen)

- » **i:** Ignore case for search pattern.
- » **v:** Invert matching, so this will display lines of the results that do not include the search pattern.
- » **-L:** Instead of showing matches, show the filenames of the files that do not contain a match.
- » **-l:** Instead of showing matches, show the filenames of the files that contain a match.

## *shutdown*

To shut down or reboot your computer, you use the `shutdown` command. This command requires that you input a time to shut down and whether you want to shut down or reboot the computer. Here is an example of rebooting immediately and shutting down (halt) the computer after 30 minutes:

```
shutdown -r now
shutdown -h 30
```

## *pwd versus passwd*

These commands are often confused with each other. `pwd` refers to *present working directory* and displays the current directory, while `passwd` refers to the password command, which is used to set a user's password.

While the typical command shell shows you the current directory as part of the command prompt, not all systems are configured to show this. If you are using a system that is not configured to show the current directory, you will use `pwd` to display the current directory. This is important as commands will always run in the context of the current directory. So unless you are specifying the full path to files you want to copy or delete, you will want to make sure that your current directory is really the directory you want to copy files to or from, or where you want to delete files.

On a Linux computer, all user accounts are stored in the file, `/etc/passwd`, and to access properties of the password or to change the password, you use the `passwd` command. For users to change their current passwords, they only have to type **passwd**.

## *iwconfig/ifconfig*

The `ifconfig` command is used to view the status of network interfaces for standard wired network connections. The `iwconfig` command is used for wireless network extensions, like the SSID. In addition to viewing the status of a network interface, you can also disable or enable an interface with these commands.

The following commands will list all network cards and their status, disable the first network card, enable the first network card, and finally display the status of the first network card:

```
etetz@linuxvm:~/Documents$ ifconfig
eth0      Link encap:Ethernet HWaddr 00:0c:29:58:ef:6e
          inet addr:192.168.1.175 Bcast:192.168.1.255 Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe58:ef6e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:2639587 errors:0 dropped:0 overruns:0 frame:0
```

```

TX packets:308848 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:182097172 (182.0 MB) TX bytes:17306850 (17.3 MB)

lo      Link encap:Local Loopback
        inet addr:127.0.0.1 Mask:255.0.0.0
        inet6 addr: ::1/128 Scope:Host
        UP LOOPBACK RUNNING MTU:65536 Metric:1
        RX packets:250568 errors:0 dropped:0 overruns:0 frame:0
        TX packets:250568 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:23289586 (23.2 MB) TX bytes:23289586 (23.2 MB)
etetz@linuxvm:~/Documents$ ifconfig eth0 down
etetz@linuxvm:~/Documents$ ifconfig eth0 up

```

## *ps*

The `ps` command, short for *processes*, lists running processes on your computer. Common options for the `ps` command include (starting with a hyphen)

- » **a:** Shows all processes for the current terminal
- » **u:** Displays user-oriented output listing
- » **x:** When used with **a**, shows all processes running on the system

## *kill*

The `kill` command is used to close applications or processes. If you have a process that is not responding, you can use `kill` to close the process. You can use `ps` to get a list of Process IDs (PIDs) and then use that PID to close the application using `kill <PID>`. If your process still does not exit, you can issue a specific exit signal, with the strongest being `-9`, which tells the process to immediately exit.

## *cat*

Short for concatenate, the `cat` command is used to join multiple files together. While it can be used to join files together, most of the time it is used to display the contents of a file.

## *su/sudo*

As a security best practice, you should perform most actions on your computer as a standard user, which provides you with limited access to dangerous actions. On Linux computers, a super user account can be used to perform privileged actions, with the default super user account being named *root*. Other user accounts can be added to the root group to grant those users root-equivalent privileges, but it is safer to grant them su privileges by adding them to the sudoers list.

The `su` command is used to switch user accounts. When used alone, without any options, it will change your account to the root account or super user, after which all commands you run will be the same as if root was performing the action. To change over to the user, you will need to know the user's password, unless you have super user privileges. In many cases, users can switch over to root, and then switch to any user. This is helpful to temporarily gain root or super user permissions, but the problem is that you may sometimes forget to switch back to your normal account, and that is where the `sudo` command comes in.

Any users on the sudoers list (`/etc/sudoers`) or any person whose account is added to the sudo group will be able to use the `sudo` command to execute any command as root (or another user). To use the `sudo` command, simply precede the command with **sudo**. Here is an example of using `sudo` to display the contents of the system hosts file:

```
sudo cat /etc/hosts
```

After running the `sudo` command, you will be prompted for your password, and that authentication will be cached by the system for a period of time.

### *apt-get*

To make installing software easier, Linux distributions make use of package managers. There are two main packages in use depending on whether your distribution is based on Red Hat Linux or Debian Linux. Red Hat Linux distributions such as Red Hat, Fedora, and Suse Linux use the `rpm` command as the root application, while Debian-based distributions such as Debian and Ubuntu make use of `.deb` packages and the `apt` package manager. Software for your version of Linux is compiled



and prepared for a specific version of Linux and then put into a repository. Most people have their systems configured to use online repositories, which makes installing software very easy.

For Debian-based distributions of Linux, the `apt` command to install or remove software is `apt-get`. To install the nano text editor on a computer, use the following command:

```
root@linuxvm:/home/etetz# apt-get install nano
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
  spell
The following NEW packages will be installed:
  nano
0 upgraded, 1 newly installed, 0 to remove and 502 not upgraded.
Need to get 194 kB of archives.
After this operation, 614 kB of additional disk space will be used.
Get:1 http://ca.archive.ubuntu.com/ubuntu/ trusty/main nano amd64 2.2.6-1ubuntu1
    [194 kB]
Fetched 194 kB in 0s (491 kB/s)
Selecting previously unselected package nano.
(Reading database ... 256158 files and directories currently installed.)
Preparing to unpack .../nano_2.2.6-1ubuntu1_amd64.deb ...
Unpacking nano (2.2.6-1ubuntu1) ...
Processing triggers for doc-base (0.10.5) ...
Processing 2 added doc-base files...
Registering documents with scrollkeeper...
Processing triggers for install-info (5.2.0.dfsg.1-2) ...
Processing triggers for man-db (2.6.7.1-1ubuntu1) ...
Setting up nano (2.2.6-1ubuntu1) ...
update-alternatives: using /bin/nano to provide /usr/bin/editor (editor) in auto
mode
update-alternatives: using /bin/nano to provide /usr/bin/pico (pico) in auto
mode
```

To remove the nano text editor from your computer, use the following command:

```
root@linuxvm:/home/etetz# apt-get remove nano
Reading package lists... Done
```

```
Building dependency tree
Reading state information... Done
The following packages will be REMOVED:
  nano
0 upgraded, 0 newly installed, 1 to remove and 502 not upgraded.
After this operation, 614 kB disk space will be freed.
Do you want to continue? [Y/n] y
(Reading database ... 256211 files and directories currently installed.)
Removing nano (2.2.6-1ubuntu1) ...
update-alternatives: using /usr/bin/vim.tiny to provide /usr/bin/editor (editor)
  in auto mode
Processing triggers for man-db (2.6.7.1-1ubuntu1) ...
Processing triggers for install-info (5.2.0.dfsg.1-2) ...
Processing triggers for doc-base (0.10.5) ...
Processing 2 removed doc-base files...
Registering documents with scrollkeeper...
```

When installing software with a package manager, the package manager will look at any dependencies and automatically install any other required applications to support the application you are installing.

While each of the main options has several switches that are supported, the main command supported by apt-get includes:

- » **Update:** Download a list of available packages.
- » **Upgrade:** Perform an upgrade of the system.
- » **Install:** Install a specified package.
- » **Remove:** Remove a package.

## **vi**

For any Linux system compliant with the core Linux standards, you should find that it has vi installed. vi is a line-based text editor. In most cases you will likely be using Vim (Vi IMproved), but the command will be aliased with vi, so typing vi will still launch the editor.



TECHNICAL  
STUFF

Although vi is a standard Linux application, there are many other text editors you may want to consider installing and using, such as nano, which is not a line-based editor.

To edit a file with vi, review “How to Edit Files with vi” by Peter Pollock at [www.dummies.com/how-to/content/how-to-edit-files-with-vi.html](http://www.dummies.com/how-to/content/how-to-edit-files-with-vi.html).

To create a new file and edit it, use the following command:

```
vi /tmp/MyNewFile.txt
```

Once you have your file open, insert mode by typing **i**. You will be able to add as much text as you would like to the file. Once you are done, return to normal mode by pressing Esc. In normal mode, most keys on the keyboard have functions. X deletes the character before the cursor, while x deletes the character at the cursor, and dd deletes the current line.

Once you have completed your editing, you may use one of the following commands shown in [Table 1-2](#).

**TABLE 1-2 vi commands**

Command	Action
:w	Write the current text buffer to the file.
:q	Quit vi.
:wq	Write the current buffer to the file and quit.
:q!	Do not save the current buffer but quit anyway.

## **dd**

The dd command is used to copy or convert a file. When working with Linux, the term *file* is relative, as often the dd command is used to create and restore an image of a driver that you may be using with your computer. The dd command only needs two parameters: if and of. To

create an image of a drive identified by the device `/dev/hdc`, you can use a command similar to the following:

```
dd if=/dev/hdc of=/tmp/hdc-image.dd
```

## *Understanding the Mac OS*

The Mac OS has gone through some major changes over the last few years. The original version, Mac OS 1.0, remained essentially unchanged up through version 9.0. The last version of the Classic Mac OS was 9.x, which was replaced with a totally different OS, OS X, which was based on the FreeBSD OS. Versions of OS X (10.0 and up) are all named after wildcats, until version 10.9 when they started using names of iconic places in California, starting with Mavericks. When version 10.12 was released, Apple shortened the OS name from Mac OS X to macOS. The latest version of macOS is 10.14 Mojave.



**FOR THE  
EXAM**

The first nine revisions of the Mac OS were proprietary, built entirely by Apple. OS X (macOS) and later are based on a FreeBSD core with Apple proprietary enhancements. The A+ exams will only deal with OS X (macOS), and so does this book; in this book, all versions of the OS X will be referenced as macOS, while Mac OS may be used to generically refer to an OS made by Apple.

### *Comparing versions of Mac OS*

The Mac OS originally hit the scene in 1984, running on a hardware platform that was very different from the hardware that was used by Windows PCs. It was standardized on the Motorola 68000 processor, and PCs were using Intel processors. The Macintosh also used Small Computer System Interface (SCSI) hard drives, and Windows PCs were using Integrated Drive Electronics (IDE) drives.

Through most of the 1990s, Mac OS 7.x was the main Macintosh OS. Shortly after the release of Mac OS 9.1 in 2001, Apple also released

macOS, with the goal of allowing capable computers to dual boot these two OSes. Unlike Windows, Apple allowed you to dual boot the old OS to run any applications that did not work with macOS rather than having to support legacy Mac OS 9 applications in macOS. macOS also offered to run old applications in an emulator called the *Classic* environment, which can be slow and requires that you have a Mac OS 9.1 system folder on your hard drive. Most Mac users were forced to quickly upgrade their applications to new versions or new applications that worked with the new macOS.

This change in OSes and the break with the previous OS allowed Apple to create a new, stable OS platform for the Macintosh product line.

In addition to a major change in the software, Apple also changed its underlying hardware and switched away from Motorola processor and SCSI hard drives in favor of Intel-based processors and SATA hard drives and SSDs.

### ***Typical system requirements***

Unlike Windows, Linux, and UNIX — which can run on a wide variety of hardware, as long as it is IBM PC-compatible — Macintosh has always run on proprietary hardware with carefully managed BIOS and system ROMs. Until recently, these systems had always been powered by Motorola and IBM CPUs, starting with the 68000 family and more recently the Power PC G5 chip. Because of the processing requirements, macOS requires at least a G3 processor to function.

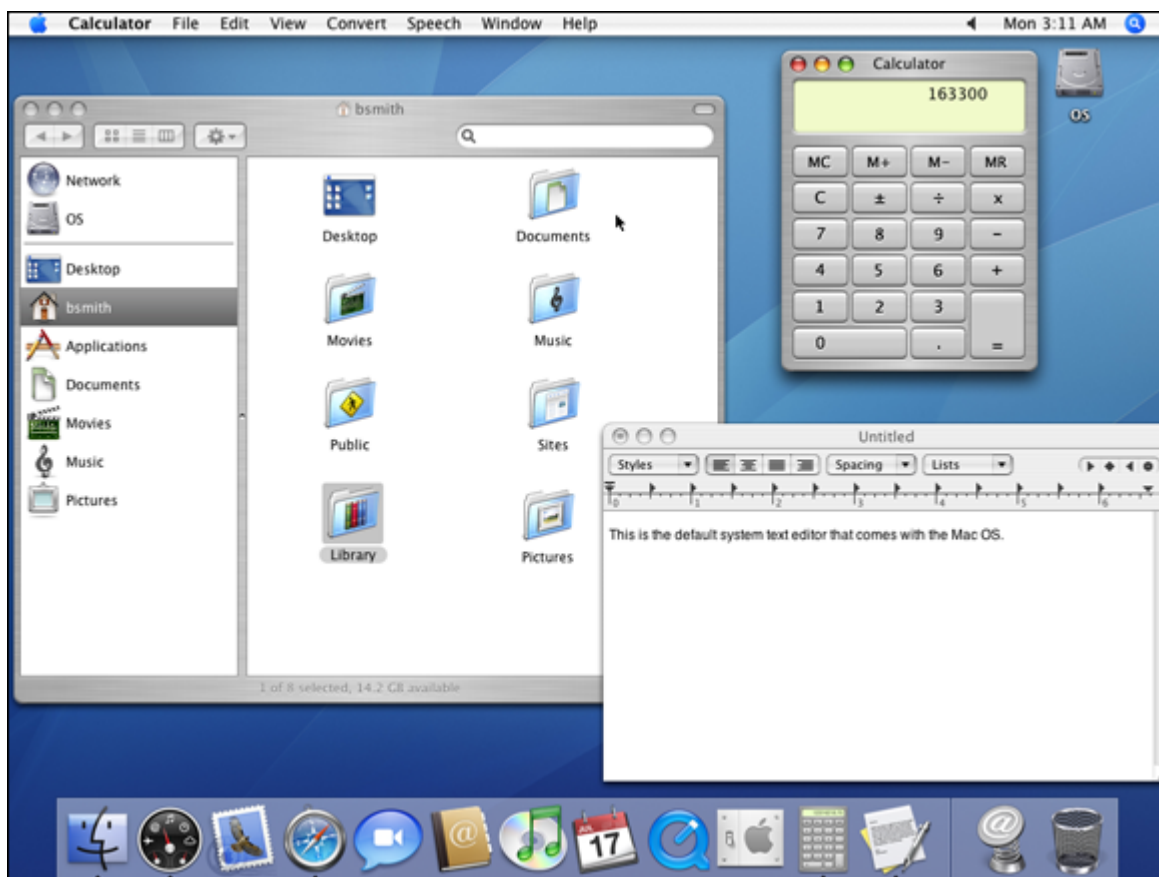
Apple switched to using Intel-based 32-bit and 64-bit CPUs in its product line, which is yet another standard component PC hardware platform, blurring the line between the Macintosh and the PC hardware platforms.

### ***Identifying GUI elements***

Prior to macOS, the Macintosh desktop environment was referred to as the *Finder* — the place where you would find all the items that you needed to work with. There were no command line interfaces for the OS because unlike other OSes, the macOS was developed from the beginning as a graphical OS.

With the adoption of the BSD-like kernel, the system added a powerful command line interface based on UNIX to a powerful Apple-developed GUI, which is still referred to as the *Finder*.

As shown in [Figure 1-6](#), the same features present on the Windows and Linux OS user interfaces are present on the macOS. One difference (or as a Mac user would think, one thing that is the same) is the Apple menu and the context-sensitive menu bar across the top of the screen. Unlike other OSes, which keep application menus with the application, Macintosh has always had a menu bar across the top of the screen. The Apple menu (the equivalent of the Windows Start menu) is always there, and the remaining menu items change based on which application has the current focus.



**FIGURE 1-6:** The Macintosh GUI for macOS.

## *Using key macOS features*

The macOS has several key features of which you should be aware. These include but are not limited to the following:

- » **Multiple Desktops/Mission Control:** Support for multiple desktops enables you to have two environments with critical desktop icons left in place. Mission Control is the tool that enables you to configure your desktop environment. You can easily change between desktop sessions by swiping up with three fingers on your touch pad.
- » **Keychain:** The macOS Keychain is a system component that stores login and authentication information for the current user. When you first need to access the Keychain after a logon, you will be asked to provide the password to unlock the Keychain and give you OS access.
- » **Spotlight:** To search for files or applications on your macOS, you are able to use the Spotlight, which looks like a magnifying glass in the top-right corner of the desktop. Spotlight is not limited to your computer, but it will also check the App Store and the Internet for applications.
- » **iCloud:** Apple provides all users access to iCloud, which is Apple's online cloud-based storage service. iCloud provides users access to basic file editing capabilities with the Notes, Pages, Numbers, and Keynote applications. In addition to these applications, you are able to store and access files in iCloud, access an iCloud email account, and use Find My Device (typically your iPhone). Most Apple iOS devices allow you to back up to iCloud. Apple provides 5GB of space for free and allows you additional storage for a fee.
- » **Gestures:** As with most laptop touch pads, the Mac laptop touch pads support multi-touch capabilities, which means it can track and support multiple fingers touching the touch pad at that same time. This allows for additional flexibility and functionality. Common gestures include
  - **Scroll:** Drag two fingers up and down
  - **Zoom In/Out:** Pinch thumb and index finger together or move apart
  - **Click:** Tap with one finger
  - **Secondary Click:** Tap with two fingers
  - **Rotate:** With thumb and index finger slightly apart, twist to the left or right

- » **Remote Disc:** The remote disk feature enables a Mac computer that does not have an optical drive to remotely use a drive from another Mac or Windows computer. To set your computer up to share a drive, enable DVD or CD Sharing in the Sharing setting of System Preferences. To access the drive from another computer, you will be able to browse for it in the Devices section of the Finder window.
- » **Dock:** At the bottom of the screen you will find the Application Dock. Similar to the Windows Taskbar, all running applications will display an icon in the Dock. Additionally, any application can be dragged to the Dock to make it available to be launched quickly and easily.
- » **Boot Camp:** To support multiple OSes, such as running Windows directly on the Mac hardware, Apple provides a boot manager named Boot Camp. When booting your computer, Boot Camp enables you to choose to load either the macOS or the Windows OS. This functionality allows you to run Windows applications on an “as needed” basis when a compatible application does not exist for the macOS. This is an alternative to running a version of Windows in a hypervisor such as Parallels Desktop or VMware Fusion, as the hypervisor solution does not always meet every person’s needs.

## *Working with key OS tools*

In addition to the OS features discussed in the previous section, many tools in the macOS are designed to make your life easier. These include

- » **Time Machine/Backup:** The main backup tool for the macOS is Time Machine, which was introduced with macOS Leopard. To use Time Machine, select a disk available to your computer and grant Time Machine exclusive access to the disk or partition. Once this is done, Time Machine automatically backs up data on an hourly basis. Time Machine will back up all your files and will then back up any changes to those files during successive Time Machine cycles. This provides an easy-to-access backup system. To retrieve old files, simply navigate to the folder that has the files you want to restore and select Time Machine from the toolbar. This launches Time Machine and shows you all previous versions of the files in that folder.



- » **Snapshot/Restore:** Snapshot is part of the Time Machine process. Once a day or every 24 hours, Time Machine generates a daily snapshot to the system drive. In addition to the daily snapshot, Time Machine also creates a weekly snapshot. These snapshots are created when the Time Machine backup drive is not available and fills in holes that would otherwise exist in the backup schedule.
- » **Image Recovery:** If you have large enough issues with your Mac, you may need to recover it or re-install the OS. Apple has integrated this process into the computer. To access the Recovery OS, press  $\text{⌘} + \text{R}$  after turning the computer on, and hold the keys until the Apple logo appears on the screen. From the recovery screen you will be able to:
- Restore your Mac from a Time Machine backup
  - Verify or repair your local disks
  - Use your Internet connection and Safari to further diagnose your problem and get help
  - Install or re-install the macOS
- » **Disk Maintenance Utilities:** All the disk utilities you should need to use with your Mac computer can be found in the Disk Utility application. Disk Utility can be accessed from the Install DVD for macOS or from the Utilities system folder, which is accessed by pressing  $\text{Shift} + \text{⌘} + \text{U}$  from the Finder interface.
- » **Shell/Terminal:** As mentioned earlier, the macOS is now built onto FreeBSD kernel, which means that underneath everything else, you are running UNIX. The fallback interface for a UNIX system is the command shell, which is accessed through a terminal application. The default terminal application for the macOS is Terminal. To find it, use Spotlight, select Finder on the Dock, and then select  $\text{Go} \Rightarrow \text{Utilities}$  to open the Utilities folder. Once in the Utilities folder, locate and select Terminal. Alternatively, press  $\text{Shift} + \text{⌘} + \text{U}$  to open the Utilities folder and locate Terminal in the folder.
- » **Screen Sharing:** Where Microsoft Windows has Remote Desktop Protocol (RDP), Apple has Screen Sharing. Screen Sharing enables you to run programs on a Mac computer while sitting at another

computer. To enable the Screen Sharing, select the Apple menu ⇒ System Preferences to open the System Preference window, and then select Sharing. Check the box in front of Screen Sharing in the list of services.

- » **Force Quit:** It is not uncommon when you are running applications to have one of them become unresponsive. When this happens, you will need to terminate that application, which is done with the Force Quit application. To access the Force Quit application window, press ⌘ + Option + Esc, choose the application you want to quit, and press the Force Quit button.

## *Implementing macOS best practices*

When working with your macOS, there are many best practices that should be followed. These practices (not necessarily limited to the macOS) include

- » **Schedule Backups:** Time Machine enables you to schedule backups. To get the most out of scheduled backups, the disk to which you are backing up should be always available to the OS. Scheduling backups is the best way to ensure that your data isn't lost.
- » **Schedule Disk Maintenance:** To keep your computer in optimal performance, you should perform regular defragmentation. There is no schedule built into the Disk Utility, so you should plan to run this tool on a weekly or monthly schedule to ensure that issues are kept at bay.
- » **System Updates/App Store:** The macOS makes use of the App Store to provide easy updates to store applications. Whenever possible you should choose applications for your computer from the App Store, as this interface makes it easy to keep these applications up to date. If you choose non-App Store applications, you will need to manage those updates separately. Operating System Updates for macOS upgrades are also available from the App Store: Just select Apple menu ⇒ App Store, and then select Updates in the title bar.
- » **Patch Management:** macOS patches are available through the Software Update tool, which is found in the Apple menu. This tool is

used to install OS patches. You will also find a list of updates in the App Store. Select Apple menu ⇒ App Store, and then select Updates in the title bar.

- » **Driver/Firmware Updates:** Driver and firmware updates for Apple-provided drivers are found in the App Store, and these are accessed in the same way you access system updates and patches: Select Apple menu ⇒ App Store, and then select Updates in the title bar.
- » **Antivirus/Antimalware Updates:** Apple does not provide a built-in Antivirus/Antimalware tool. These updates are critical to your system. Most third-party tools have built-in options to schedule updates, which you should enable so that security updates are automatically applied.

## *Difference and Similarities between OSes*

You have now looked at the Windows, Linux, and Mac OSes. You should be now be familiar with the key areas where these different OSes are different and where they are the same. In all cases, there is support for an easy-to-use GUI front end, while in some cases that front end is carefully crafted and controlled by the manufacture; in other cases, it can be freely modified and enhanced by any programmer with the desire to. While some OSes offer features that are unique, in most cases, the best features show up in all OSes.

### *Vendor-specific limitations*

While there are often hard limits in life, there are also often soft or self-imposed limits that exist as well. An example of this could be a pair of jeans. You wear the jeans daily for a year, and start to notice that they have worn in several areas and are no longer a nice dark blue. Are they still functional? Yes. You wear them for another year and notice that they have a worn through in the knee and have started to rip. Are they still functional? Maybe. As jeans, they are still functional, and will keep you clothed, warm, and out jail for public exposure, but since you wear them

to work or social gatherings, they are no longer acceptable. This would be a self-imposed limit to the jeans. If you continue to wear them until the rip in the knees goes all the way around your leg, then you are left with shorts, and the jeans have reached a hard limit for their functionality.

Vendors impose their own limits on the products they make. They do not mean that the product is no longer functional or worthwhile, but that the product has reached a limit that the vendor is not willing to them past.

### *End-of-life*

Microsoft has a lifecycle policy, which you can find by searching for Microsoft Lifecycle Policy in your favorite search engine. Microsoft's standard policy provides support for a product for 24 months after release, which is what it calls "mainstream support." After this 24-month period, Microsoft provides up to five years of extended support. During the extended support phase of the product's life, only security patches are released for the product, no feature enhancements.

If we take a look at Windows 7, it was released in December 2009, but within two years of its release, Microsoft released Service Pack 1 for it. That release of the service pack changed the product, giving the new product its own release date of February 2011. That service pack reached the end of mainstream support on January 2015. Windows 7 will reach the end of extended support as of January 2020. After this date, Microsoft will no longer release any updates for the product, including security updates. Since Windows 8.1 was released in November 2013 and Windows 10 was first released in July of 2015, there has been plenty of time for users to migrate to a newer operating system. Although since Windows 8.1 is already in extended support, it would make sense that those upgrades should be to Windows 10.

Windows 10 has a much shorter end-of-life, which is now typically 18 or 30 months (depending on edition and month of the release), but the upgrade process is now almost as simple as applying your monthly updates.

### *Update limitations*

Microsoft has a policy on updates, and when looking at Windows 10, this becomes very clear. Microsoft offers updates to the currently supported OSes. Once you pass the 18-month limit on the OS, and you exceed the end-of-life, you are no longer offered updates. In order to receive security and feature enhancements, you are required to upgrade to the latest release of Windows 10.

You see similar support in products like Apple's iPhone, where your hardware may be sufficiently old that it will not offer you the latest OS, as it may not operate on your hardware in a manner which Apple desires for you to have a positive consumer experience.

### *Compatibility concerns between operating systems*

If you look around most organizations, you will find that they have standardized on one OS platform, either Windows, Mac, or Linux. This standardization within the organization means the IT group within the company only has to learn one platform, and only needs to support one platform. It also means that there should be no compatibility issues between systems.

When mixing devices with different OSes, you will often need to find some common ground to allow for communication, but even then the devices will not operate like devices native to that technology. So while you may be able to have a Mac join a Microsoft Active Directory domain and save its files on a Windows server, it does not process Active Directory policies or run logon scripts. When mixing devices from different OSes, you need to be aware that there will be some limits to what you are able to do.

It is not enough to worry about compatibility within your company; you likely communicate with other companies, so you will want to ensure that there is some compatibility between your company and theirs.

## *Choosing an Optimal System*

A computing system can have many different roles, and depending on the role, you will want to choose your hardware appropriately. In this

section, you take a look at the most common types of systems that you will likely encounter, and the types of hardware that will best suit those roles.

### » **Graphics/CAD/CAM workstation**

- This type of system is used for graphic design work and requires high-performance components.
- Powerful processor, dual or quad core.
- High-end video card.
- Maximum supported RAM for the motherboard.
- SSD for optimal disk access speed.

### » **Audio/video-editing system**

- Similar to graphics-based systems, these systems also require high-performance components, but specifically focus on A/V components.
- Specialized audio and video card to support capture and editing.
- Large, fast hard drive to store content and manage processing.
- Dual monitors.

### » **Virtualization workstation**

- To virtualize and run multiple instances of the Windows, Linux, or macOS, your computer requires the equivalent of multiple computers' worth of processing speed and memory.
- Maximum RAM supported by the motherboard.
- Multiple processor cores and multiple processors.

### » **Gaming system**

- Similar to graphics systems, a gaming system requires specific components to support graphics-intensive gaming applications.
- Powerful processor, multiple cores if games benefit from them (however, not all games make use of multiple cores).

- High-end video system, including specialized GPU to support fast-paced screen presentation.
- High-end, high-definition sound card.
- High-end cooling to support the heat generated from system components when gaming is taking place.
- SSD for optimal disk access speed.

#### » **Network-attached storage device**

- Media streaming for playback of saved media to remote devices.
- File sharing for networked devices.
- Gigabit NIC to provide optimal access speed for networked devices.
- RAID array provides safety for your disk data in the event of disk failure.
- Hard drive of a large and sufficient size to support your data storage needs.

#### » **Home theater system**

- Theater systems need graphics power to drive large monitors and audio support to provide surround sound.
- Surround-sound audio for movie playback.
- HDMI output for integration with home theater components.
- HTPC compact form factor to have integrated appearance with other home theater components.
- TV tuner for TV viewing and recording.

#### » **Media streaming front-end system**

- With the number of streaming services available today, many people are opting for small front-end devices rather than powerful home theater systems. Size is often the factor here, with the smallest being devices such as the Raspberry Pi (GETURL).

- Meets requirements for hosting OS.
- Network connectivity.
- HDMI port for easy connectivity to televisions.

#### » **Standard thick client**

- The standard office computer designed to run desktop applications.
- Meets or exceeds the recommended requirements for running the selected OS.

#### » **Thin client**

- Thin-client computers are not designed to run major applications, but rather to run applications through a remote session on a server. Locally, they only need to support basic applications, such as a web browser.
- Meets minimum requirements for running Windows or the hosting OS.
- Network connectivity to access the server hosting the desktop session.

#### » **Home server PC**

- Home servers do not require high-end audio and video components, but rather serve data stored on hard drives to other computers over the network.
- Media-streaming, file-sharing, and print-sharing OS components.
- Gigabit networking to provide access for multiple client devices.
- RAID array and disk system provides reliable storage for files.

When it comes to working with your desktop computer, there are a few things to consider. When working with your desktop, you may be part of a domain, or you may be stand-alone. In either case, you will have user accounts you are dealing with, in addition to user and device settings.



You may be using a thin or thick client, and the user accounts you are using may be found on the client device or in Active Directory. If you are using a thin client, you may not have a local account on the device you are using, but rather only have a user account on the virtual desktop client to which you are connecting.



**TIP**

When dealing with user account setup and settings, you need to consider where these accounts will be set up, and where they will be used.

## *Getting an A+*

This chapter shows the differences between the major operating systems on the market — Windows, Linux, and macOS. Things to remember include

- » The major operating systems are Windows, Linux, and macOS.
- » Windows and Linux hardware is compatible, but applications are not.
- » Linux comes in subvarieties called *distributions*.
- » The OS you are using may have limitations related to updates, lifespan, and support.
- » All three OSes have similar GUI environments.

## *Prep Test*

**1. Mary works for a temporary placement agency and uses primarily Windows on her jobs. She is going to be sent to an office that uses macOS. Should Mary expect to have large problems getting used to the new OS?**

(A) Mary should expect to find the layout of the screen and the method of accessing applications to be completely different.

- (B) Mary should refuse to visit the client site because the differences are so great.
- (C) Mary should expect to find the layout of the screen and the method of accessing applications fairly similar to what she is familiar with.
- (D) This is a moot point because the GUIs on both operating systems are identical.

**2. You have been called by a client to give a recommendation on which OS should be installed on several new computers being added to the office. The other computers in the office use Windows-based clients (Windows XP) and Windows-based servers (Windows 2003). What OS should you suggest?**

- (A) Red Hat Linux
- (B) FreeBSD Unix
- (C) macOS
- (D) Windows 10

**3. Which of the following operating systems are direct ancestors of Windows 7? (Choose all that apply.)**

- (A) Windows 2000
- (B) SUSE Linux
- (C) Windows NT
- (D) Windows Me

**4. What is the variety of packaging of the Linux kernel and applications called?**

- (A) Conglomeration
- (B) RPM
- (C) Revision
- (D) Distribution

# Answers

1. **C.** Mary should find that the interface is different, but not so different that she cannot accomplish her tasks. If she wants to develop as high a level of competency as she possibly has with the Windows OS, training would be beneficial but not required. See the “[Identifying GUI elements](#)” section of “[Understanding the Mac OS](#).”
2. **D.** Because the office is already Windows based and the users likely have a higher degree of proficiency with the new version of the Windows OS, a change to a more different OS should not be implemented unless the client has some specific goal that he wants to achieve by switching the OS. Even though, with the changes that have occurred with Windows 10, when compared with Windows XP, the user might be able to pick up any of the suggested OSes with the same level of difficulty. Review “*What Is an Operating System?*”
3. **A, C.** Windows NT and Windows 2000 have a common heritage with Windows XP in that they all use NT technology. Windows 9x operating systems, such as Windows Me, followed a different development path going back to Windows 3.0. Check out “[Comparing versions of Windows](#).”
4. **D.** A distribution includes packaging of the Linux kernel, and applications. It usually also includes a package of management tools and a system installation program. Peruse “[Comparing Linux versions](#).”

## Chapter 2

# Windows Operating System Functions

---

### IN THIS CHAPTER

- » Identifying the primary operating system components
  - » Describing operating system interface features
  - » Using Remote Desktop Connection and Remote Assistance
  - » Working with virtualization
  - » Identifying cloud concepts and cloud services
- 

Just as the engine is the driving force behind an automobile, the operating system (OS) is the driving force behind your computer. Your choice of engine in your automobile affects the performance of its system, and also affects what you can do with your vehicle. In a similar way, you will find that the performance and functionality of your computer are different if you use MS-DOS, Windows 8.1, Windows 10, or some other OS.

The OS is responsible for several major functions on your computer. To manage your computer, the OS relies on its major components. This chapter examines these components and how they interrelate to effectively manage the computer. By the end of this chapter, you will be able to effectively choose from Windows 7, Windows 8.1, and Windows 10 for your system. And because the A+ exams focus on Windows 7, Windows 8.1, and Windows 10, this chapter focuses on these three OSes.

## *Identifying Major Operating System Functions*

As you read in the preceding chapter, the OS is responsible for two major functions: managing hardware devices and providing an environment in which applications can execute. One of the major applications that needs to execute is the user interface (UI), which lets users control all other applications and their execution. In the case of Windows-based computers, this UI — the *shell* — is Windows Explorer. So together with hardware, this software that makes up the OS is responsible for getting things done. The hardware and software get tied together in the location where everything happens: memory.

## ***Understanding memory management***

Memory is the playing field where hardware and software mix. Memory management is the responsibility of the OS. The OS makes sure that the hardware and software components work within their own confines of memory. As memory resources are requested, the OS releases them either to the hardware device driver or to the application. The OS then takes steps to make sure that the application accesses only the memory areas allocated to that particular application. If an application attempts to access memory not allocated to it, the OS has to decide what to do with the application, which is to deny access to the memory.

As part of memory management, the OS keeps track of physical memory on the computer as well as hard drive space used as extra memory available to the computer. Access time to physical memory is measured in nanoseconds, and access time to disk drives is measured in milliseconds. These scales are widely different, and so is the access time of information from these memory locations. Both types of memory are lumped together to make up virtual memory. Sometimes the term *virtual memory* is applied to the hard drive space used to simulate memory, but at the OS level, the term is used to refer to all memory available for storage on the system.

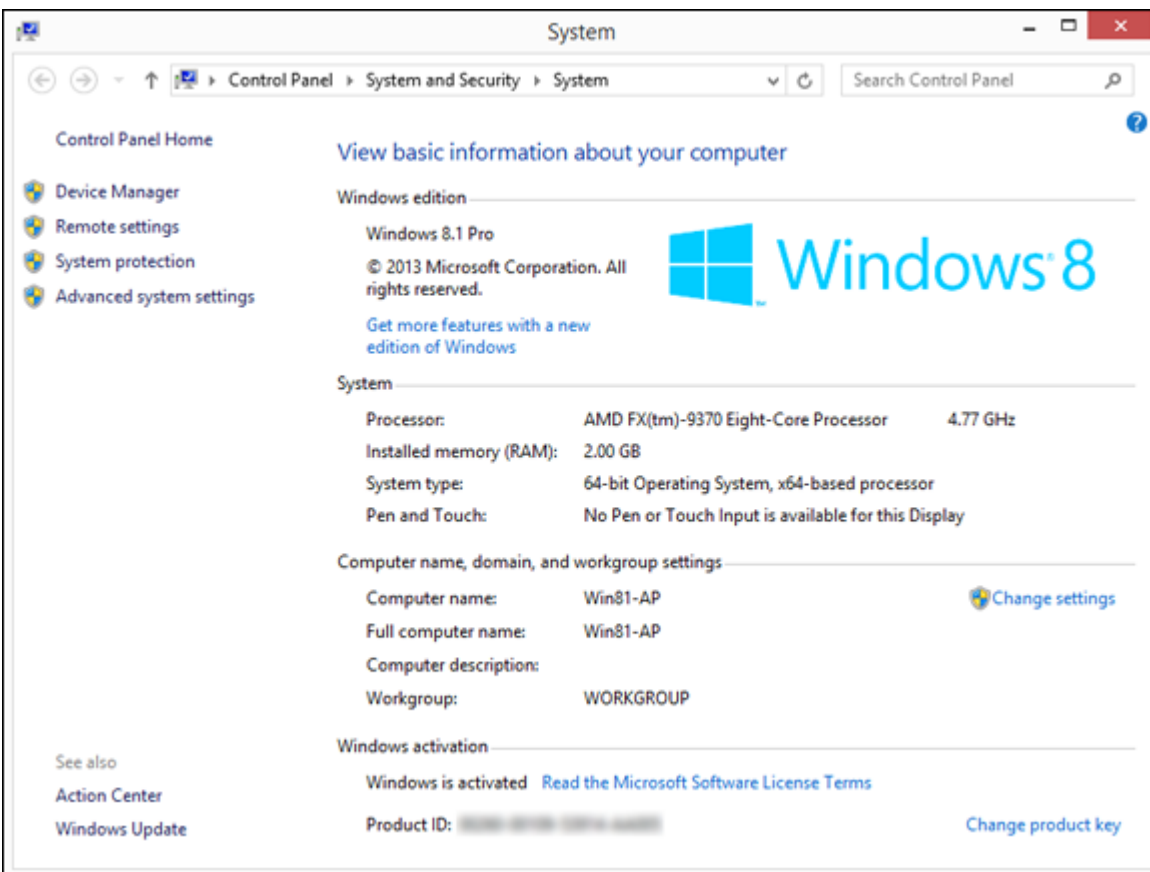
As applications launch and get loaded into memory, physical memory is used. When this space becomes limited, the OS moves some data from RAM onto the hard drive. The OS records the change in the actual location so that when the application requests that information again, the information can be moved back into physical memory and accessed.

## Checking the OS version

No matter which OS you use, at some point you need to know its exact version number. This is often the case when you install new software, which requires a specific version of the OS. There are many methods for retrieving this information in Windows.

The System Control Panel or System Properties lets you know which version and service pack level of the OS you are running (see [Figure 2-1](#)). You can get to the System Properties dialog in the following ways:

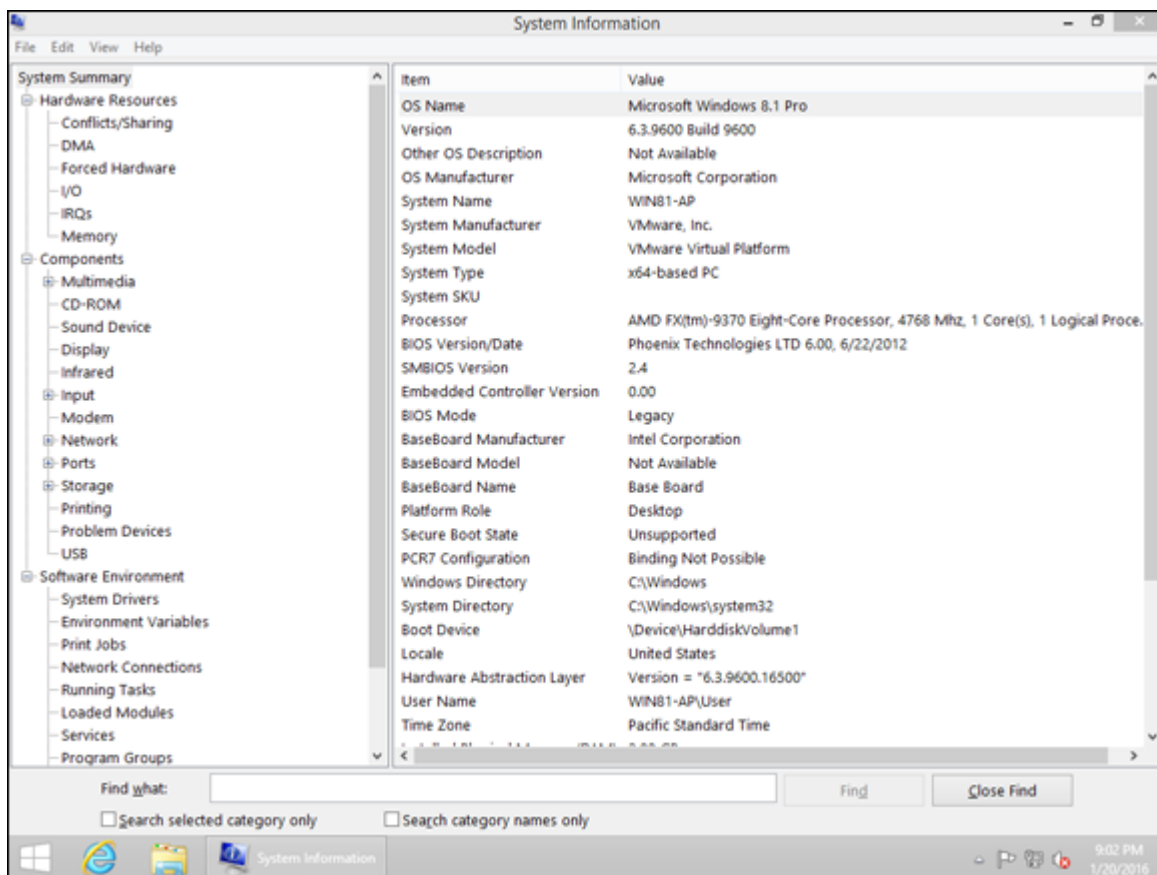
- » Choose Start ⇒ Control Panel ⇒ System.
- » Right-click Start and choose System.
- » Right-click Computer or This PC and choose Properties.



**FIGURE 2-1:** The System Control Panel is available in all versions of Windows.

System Properties will show you the version name, like Windows 7 or Windows 10, but starting with Windows 7 and newer OSes you need the System Information tool to locate the version number. To see this information in the System Information tool in Windows 7, choose Start ⇒ All Programs ⇒ Accessories ⇒ System Tools ⇒ System Information.

The System Information tool includes the version number in the main window (see [Figure 2-2](#)). The System Information tool can be launched through the Start menu prior to Windows 8.1, but in all versions of Windows you can use the Run command and type **msinfo32.exe** or choose Start and type **msinfo32.exe**.



**FIGURE 2-2:** The System Information tool for Windows provides a great deal of detailed information.

Some of the version numbers you might see are listed in [Table 2-1](#). Notice that these version numbers are continuations of Windows NT version 4.0 in version and build numbers.

**TABLE 2-1 OS Version Numbers for Modern Versions of Windows**

<i>Operating System</i>	<i>Version Number</i>
Windows NT 4.0 Workstation	4.00.1381 Build 1381
Windows 2000 Professional	5.00.2195 Build 2195
Windows XP Professional	5.10.2600 Build 2600
Windows Server 2003 Enterprise	5.2.3790 Build 3790
Windows Vista Enterprise	6.0.6000 Build 6000.16386
Windows Server 2008 Enterprise	6.0.6000 Build 6000.16386
Windows 7 Enterprise	6.1.7600 Build 7600
Windows Server 2008 R2 Enterprise	6.1.7600 Build 7600
Windows Server 2012	6.2.9200 Build 9200
Windows 8.0	6.2.9200 Build 9200
Windows Server 2012 R2	6.3.9600 Build 9600
Windows 8.1	6.3.9600 Build 9600
Windows 10 Version 1507	10.0.10240 Build 10240
Windows 10 Version 1511	10.0.10586 Build 10586
Windows 10 Version 1803	10.0.17134 Build 17134
Windows 10 Version 1809	10.0.17763 Build 17763

Windows version numbers have three parts: the version number, the build number, and the Service Pack level (although not all tools will show you the Service Pack level). The version number (6.1 for Windows 7) will not change for the lifetime of the product. As patches and upgrades become available for the OS, Microsoft releases hot fixes. *Hot fixes* are listed in the Programs and Features Control Panel. When a sufficient number of fixes have been released, Microsoft releases a Service Pack, which incorporates most hot fixes as well as other unreleased fixes or features.

Windows changes the build number of the OS as you apply service packs or cumulative updates in Windows 10. The two major parts of the build number do not change, so for Windows 10 they will remain as 10.0; the



two minor parts of the build number change, so the minor version number for Windows 10 Version 1809 with March 1, 2019 Cumulative Update is actually 17763.348, where 17763 identifies Version 1809 and 348 is the hotfix level within that version.



TECHNICAL  
STUFF

[Table 2-1](#) does not include all Windows 10 versions, but you can see the first two versions and the last two versions (as of the writing of this book). Microsoft recently announced that it will make two releases a year: once in the spring (xx03) and once in the fall (xx09), where the version number will be made up of the year and month of the release. The major build number will remain consistent for the release, but the minor number will change with cumulative updates and hotfixes. You can see all version update information for Windows 10 at <https://support.microsoft.com/en-us/help/4099479/windows-10-update-history>.

After you know which version of the software you are running, you can take a look at what makes up your OS.

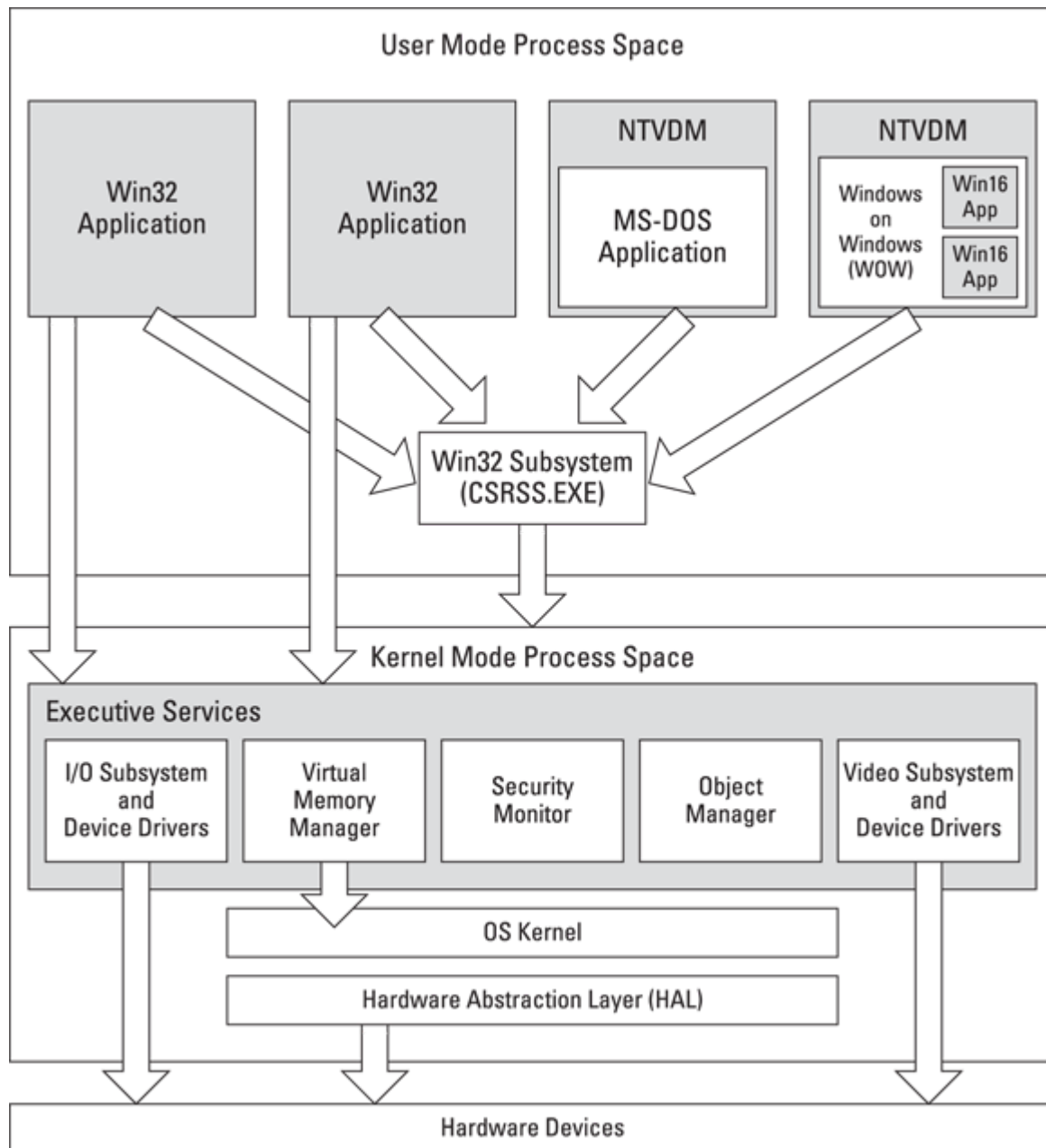
## *Understanding Major Operating System Components*

In the following sections, you briefly examine how applications actually run on Windows computers. For a more complete description of how applications are supported, see Book 6, [Chapter 2](#).

### *Getting into the architecture*

Windows 2000 was a complete rewrite of the Windows OS, but at a risk of causing compatibility issues. When Windows boots, it immediately enters a 32-bit protected-mode or a 64-bit long-mode state. With a 32-bit processor, the entire OS operates from this 32-bit state, and the kernel is loaded into *Ring 0*, which Microsoft refers to as *kernel mode* (see [Figure](#)

2-3). All processes running in kernel mode are protected from any processes running in *Ring 3*, or *user mode*.



**FIGURE 2-3:** The Windows architectural overview.

The Intel processor design divides operation of the code into four separate execution levels, called *rings*. Ring 0 is at the middle of this arrangement, and Ring 3 is at the outside. These are the only two rings that Microsoft implemented during the development of 32-bit Windows OSes

and this has continued with the implementation on 64-bit processors. When working with 64-bit Windows OSes, the only difference is that the underlying subsystems are 64-bit, and a simulated 32-bit environment is provided for 32-bit applications.

The kernel is the core part of the OS that controls everything else that happens on the computer. The kernel is responsible for keeping user-mode processes separated. Each application is started in its own area. One application is not directly allowed to interact with other applications and must pass such requests through *Executive Services*, which operate in kernel mode. This isolation of the applications from each other and from the rest of the OS is one of the keys to the stability of the current Windows system.

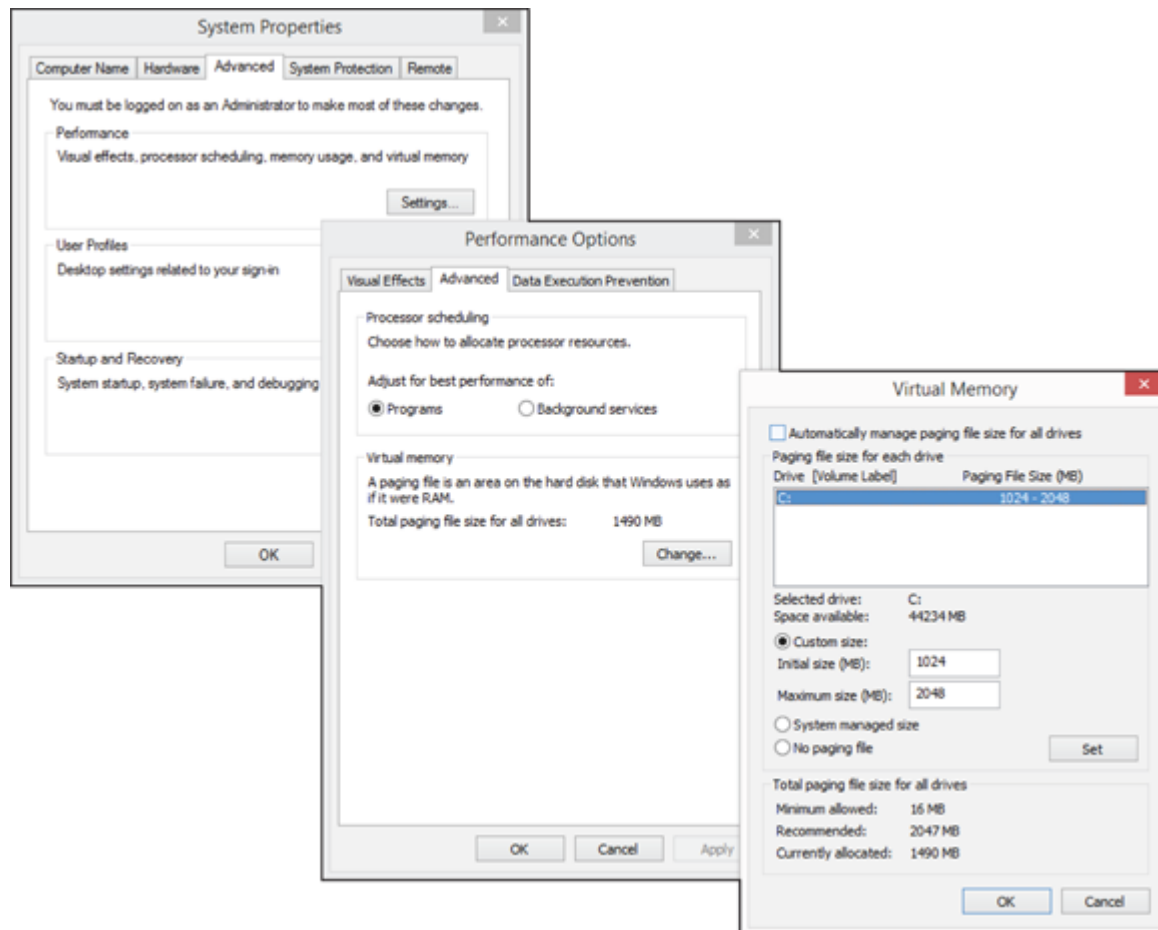


TECHNICAL  
STUFF

Kernel-mode processes are separated from user-mode processes but are vulnerable to corruption by other kernel-mode processes. The processor's architecture is all that protects kernel-mode processes from each other, and it often fails in its job. This means that Stop events (the ones that cause the infamous Blue Screen of Death), which reboot the system, are usually caused by a conflict of the processes running in kernel mode. For more on Stop events, see Book 7, [Chapter 2](#).

## *Paging your memory*

Windows uses hard drive space to extend the amount of memory available to applications. The total pool of available memory is the *virtual memory page pool*, or just *virtual memory*. Virtual memory, composed of physical RAM and hard drive space, is maintained by the Virtual Memory Manager (VMM). [Figure 2-4](#) shows how these systems relate.



**FIGURE 2-4:** A sample of virtual memory within the Windows 8.1 OS.

The VMM is responsible for keeping track of where different kinds of information are located in memory. As applications request to have information placed in memory, the VMM places the information in an area of RAM. If RAM is getting full, some information is moved from RAM to an area on the hard drive. The location on the hard drive is a *swap file* (in older version of Windows) or a *paging* or *page file* (current versions of Windows). As applications request stored data, the VMM moves information so that the data is available in RAM.

You configure the paging file in the System Properties. You might want to adjust the virtual memory settings because

- » You are running out of space on your boot partition (the one with the Windows directory).
- » You want to improve paging performance by

- *Reducing disk contention with the OS:* In this case, you can move the paging file to a different physical disk if you have one.
- *Load balancing the page file between different physical drives:* Current Windows systems allow you to have multiple paging files, each on a different disk.

Follow these steps to adjust how much virtual memory your computer uses when using Windows:

**1. Open the System Properties dialog box by right-clicking the Computer on the Start menu and choose Properties, and then select Advanced System Settings.**

**2. In the System Properties dialog box, click the Advanced tab.**

**3. Click the Performance Settings button.**

The Performance Options dialog box appears.

**4. On the Advanced tab, click the Virtual Memory Change button (refer to [Figure 2-4](#)).**

In the Virtual Memory dialog box that appears, you can set an initial and a maximum size for the paging file on each logical drive.

**5. Adjust the settings as needed.**



**TECHNICAL  
STUFF**

If you reduce the size of the paging file on your boot partition below the size of the physical RAM on your system, you are warned that some of the recovery options will be disabled. The paging file is used as a storage space for the `memory.dmp` file that is generated during a Stop error. As long as you have not undersized your boot partition, you should not have to worry about this too much, but in some environments, such as virtual machines, it is not uncommon to have the boot partitions undersized.

**6. Click OK on three consecutive dialog boxes to close them all.**

## Choosing your file systems

Just as many companies have different systems for filing data, with Windows you have several options when choosing a file system. MS-DOS offers the File Allocation Table (FAT), which started out as FAT12 and then became FAT16 in later versions of MS-DOS. Windows 95 then added to that base file system with FAT32. In between this time, the different architecture of Windows NT offers the New Technology File System (NTFS). The latest versions of Windows support all three file systems, and you get some control over how to use them.

When using Windows, your choices include FAT, FAT32, and NTFS.

[Table 2-2](#) summarizes some of the differences between the file systems.

**TABLE 2-2 Differences between the Major Windows File Systems**

<i><b>File System</b></i>	<i><b>OS Support</b></i>	<i><b>Partition Size</b></i>	<i><b>Max File Size</b></i>
NTFS	All versions of Windows NT (including Windows 7, Windows 8.1, and Windows 10) support NTFS, but there were major changes to the file system with the release of Windows 2000. Computers running older versions of Windows NT might not be able to access the files.	10MB up to a theoretical limit of 16EB*	Limited only by the size of the volume
exFAT	Originally released with a version of Windows CE and making its desktop debut with Windows 7. This file system was developed as an extension of the FAT32 file system to be used on removable media and in places where NTFS is inappropriate or unusable. All current versions of Windows and Mac OS X 10.6.4 or newer Mac OSes have support for this file system.	64ZB (512TB recommended)*	64ZB (512TB recommended)*

<b>File System</b>	<b>OS Support</b>	<b>Partition Size</b>	<b>Max File Size</b>
FAT32	FAT32 was released with Windows 95 OSR2, and all versions of Windows 9x after that support FAT32. Windows 2000 was the first OS in the Windows NT family to support FAT32.	Up to 2TB,* usually used for FAT volumes larger than 512MB. Windows Vista, Windows 7, and Windows 8.1 will not format partitions larger than 32GB with FAT32.	4GB
FAT	Accessible by all Microsoft OSes since MS-DOS, including all Windows NT-based operating systems. It is also widely supported by other OSes.	Up to 4GB. MS-DOS and Windows 9x allow you to create FAT partitions only up to 2GB; Windows NT-based systems can create partitions up to 4GB.	2GB

*\*One terabyte (TB) equals approximately 1,000 gigabytes. One exabyte (EB) equals approximately 1 billion gigabytes, or 1 million terabytes. One zebibyte (ZB) equals approximately 1,000 exabytes. That's a lot of memory!*

In most cases, you want to use NTFS because it

- » Supports security on folders and files
- » Is a journaling file system, so it offers better recovery in case of power interruptions
- » Offers a more stable platform for data storage

Although some older applications might have compatibility issues with NTFS, these issues are rare. For more on file systems, see Book 2, [Chapter 5](#).



**FOR THE  
EXAM**

NTFS should always be chosen as the file system for stability and security. Choose FAT, FAT32, or exFAT only if you need to dual-

boot a computer with another OS, such as Windows 9x or Linux.

## Understanding the Registry

Windows uses its Registry to record settings for applications and the OS. When people first started writing applications for Microsoft-driven computers, they usually needed to record a series of per-use or per-computer settings. In most cases, they wrote these settings to a file stored on that computer. This system worked fine most of the time, but the people who needed to manage those computers and applications found that some of these configuration files were binary files and some were text files, and occasionally they would get corrupted and be unusable.

To solve some of this confusion, Microsoft came up with a file standard that appeared when Windows was introduced to the world. The new solution was the INI (“innie”) file, which is a text file that uses sections, settings, and values stored in a standardized format. Because data is written and can be retrieved using a standard format, the OS can use standard procedures to store and retrieve the data rather than relying on each application developer to write his or her own procedures. [Listing 2-1](#) shows a portion of a sample INI file that would have been opened in `notepad.exe`. For all text-based configuration files, you can make changes with `notepad.exe` or `wordpad.exe`.

## **LISTING 2-1 A Sample INI File**

```
[Options]
WordSel=0
Units=0
Maximized=0
FrameRect=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
PageMargin=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
DefaultFormat=5
[Text]
Layout2=CAAAAAAAAAEAAAAAAAAADAAAAAAAAA
LayoutAux2=CAAAAAAAAAEAAAAAAAAADAAAAAAAAA
Wrap=0
BarState0=0
BarState1=0
[RTF]
```



```
Layout2=CAAAAAAAAAEAAAAAAAAAAAAAAAAA
LayoutAux2=CAAAAAAAAAEAAAAAAAAAAAAAAAAA
Wrap=0
BarState0=0
BarState1=0
```



**TIP**

Section names are enclosed in square brackets.

With the release of Windows 95 and Windows NT, Microsoft programmers developed a new way to deal with this issue — they created a single location in which to store all configuration information for a computer: the *Registry*.

Like INI files, the Registry uses a standard format, breaking down settings into two basic categories: for computers and for users. Computer settings are stored in a section named `HKEY_LOCAL_MACHINE`, and user settings are stored in `HKEY_CURRENT_USER`. Application developers are encouraged to use this new location to store settings for their applications and have even been given a special software key to store their settings. It is up to the software developer to decide whether settings are user- or computer-based and to manage the settings appropriately.

All well-written programs should be using the Registry to store configuration information, but you may see INI files storing setup options for installer programs, or the similarly formatted INF files for drivers.



**FOR THE  
EXAM**

Remember that Registry stores all settings in either `HKEY_LOCAL_MACHINE` or `HKEY_CURRENT_USER`, depending on whether the setting is related to the computer or the user.

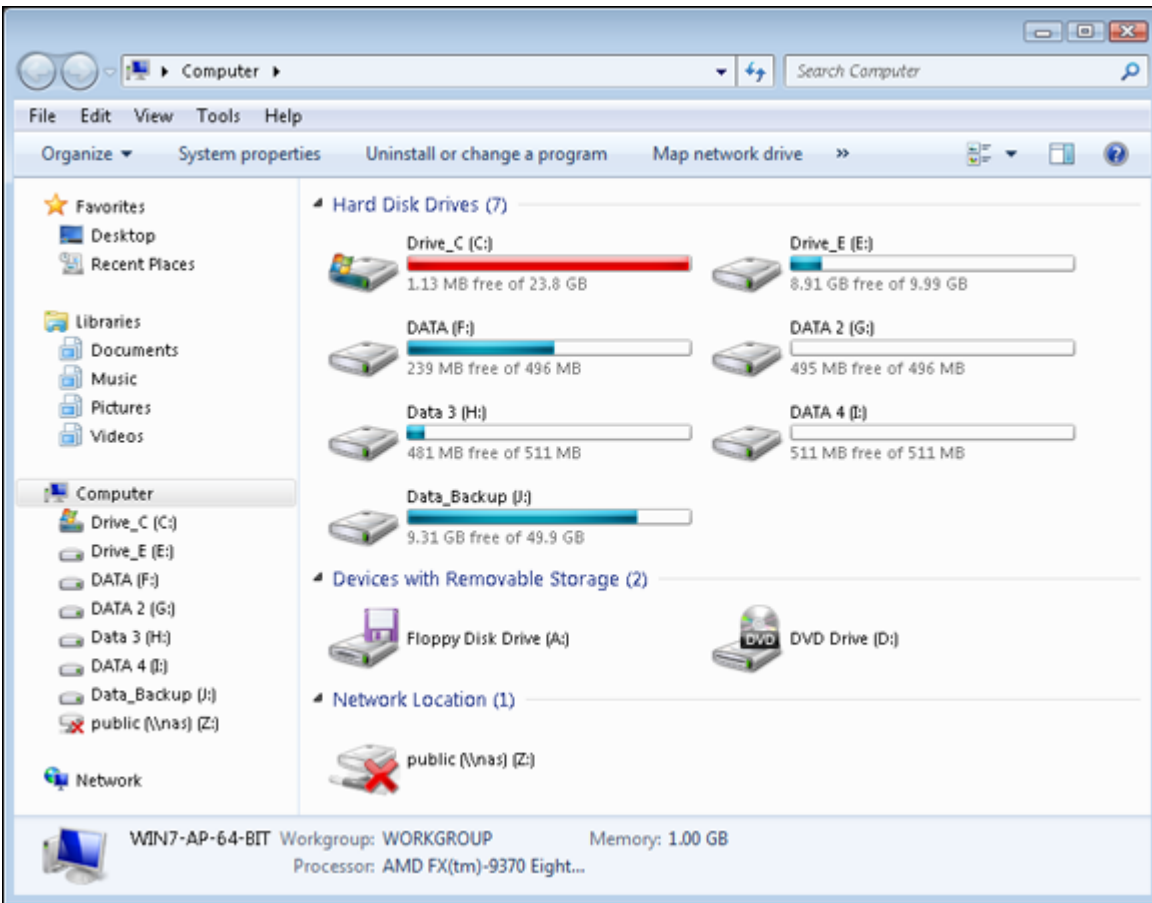
For detailed information about how to view and manage settings stored in the Registry, read Book 6, [Chapter 4](#).

# *Navigating Your Computer*

File and folder structure or paths is how you get around the disk system on your computer. Being able to get to the files you need when you need them is crucial. From the command prompt, you can work with `cd` (change directory) and `dir` (directory), which I cover at length in Book 5, [Chapter 5](#). When you are using Windows, you can choose between Windows Explorer or File Explorer (not Internet Explorer) and This PC (or Computer in Windows 7). Either tool can be used for navigation, and your choice is purely preference. This section looks at these tools in a fresh (default) Windows installation using the default settings. If you have changed your settings, some windows might not be the same as I describe. When possible, I try to describe the differences among Windows 7, Windows 8.1, and Windows 10.

## *This PC*

This PC (or Computer for Windows 7) is the most common way people access files on their computers because it's easy to find in the Start menu on Windows, or in the Folder icon on the Windows 10 Taskbar. When you click This PC, a large window is displayed (as shown in [Figure 2-5](#)), listing the drives on your computer. You can then double-click your C: drive to see what files are located on that drive.



**FIGURE 2-5:** Use This PC or Computer to navigate file systems on the drive.



**REMEMBER** The navigation buttons on the toolbar at the top of the This PC window allow you to go back to the previous folder or up to the parent folder. Cut, Copy, and Paste buttons allow you to move files between folders.



**TIP**

Several tasks are more easily accomplished with an additional open window, such as copying files from one folder to another. To open an additional window, double-click This PC on the desktop and browse to the correct folder; or, hold down your Ctrl key while you double-click a folder, which leaves the original window in place and opens a new window for the folder that you double-clicked.

If you don't like how the files in the This PC window are displayed, use the Views button on the toolbar to change the view from Icons to Thumbnails, Tiles, List, or Details. Thumbnails view allows you to see the contents of many files, such as graphics; Details view lists file sizes and modification dates, which is often useful when trying to locate specific files. The choice of viewing style is preference. Windows 7 and newer OSes add to your choice of views with Content and a variety of icon sizes (from small to extra large). Content will show details about the contents of your files, such as dimensions, file type, or size. The Thumbnails view has disappeared with the newer OSes, but do not fret, because for most graphic files, you can see the contents in the Content, Tiles, or larger Icons views.

In the address line near the top of the This PC window, you can type the name of the folder that you want to go to and directly switch to it. For example, you could type **C:\Windows** to switch to the Windows folder.

When you select an item in the This PC window, you see properties for that item at the bottom of the window in Windows. To display or hide the Preview, Navigation, or Details panes in Windows 7, choose them from the Layout submenu of the Organize menu. In Windows 8.1 and Windows 10, choose them from the View Ribbon.

To explore many of the options for displaying information in the This PC window, open the Folder Options dialog box from the Folder and Search Options from the Organize menu in Windows 7 or Options ⇒ Change folder and search options from the View Ribbon in Windows 8.1 and Windows 10.



FOR THE  
EXAM

If you open and explore the Folder Options, you will find options for browsing folders and opening folders, and how the Navigation pane will function all on the General tab. Many options are found on the View tab, including how to display files with the hidden attribute set, empty drives, system files, and file extensions. This tab also provides an option to apply these settings to all folders, as well as the option to reset folders to their default settings. There is also Search tab to adjust search settings, which include searching in system directories and displaying partial matches. To prepare for your A+ exams, it is a good idea to review the settings that can be modified in the Folder Options dialog box.

## *Windows Explorer*

By the end of this section, you will see that This PC or Computer as an application does not actually exist. To open this application in Windows, choose Start ⇒ All Programs ⇒ Accessories ⇒ Windows Explorer or choose Start, type **Explorer**, and choose File Explorer from the available choices. This opens the Windows Explorer program with the left pane — the *Navigation pane* or *Folders Explorer Bar* — enabled.

Now, you will see why a This PC or Computer application does not really exist. If you select This PC or Computer in the Navigation pane, close the navigation pane, and change the view to Icons for both Windows, you will see that this window is the same as the This PC or Computer window. To show the Navigation pane, select Organize ⇒ Layout ⇒ Navigation Pane. The Navigation pane allows you to quickly move from one folder to another, or copy files from one folder to another without opening multiple windows. Many Windows users prefer the Explorer view to the Computer view of their files.

In summary, both views of your files use the same program: Windows Explorer or `explorer.exe`.



TECHNICAL  
STUFF

`explorer.exe` is not only used for This PC or Computer and Windows Explorer. The first time it is run on your computer, it is launched as the desktop shell. If you close all open windows and check your Processes tab in Task Manager, you will see one copy of `explorer.exe` still running. If you right-click on `explorer.exe` in the processes list and choose End Process, your desktop will disappear, and you will see only your wallpaper. If `explorer.exe` does not automatically reload, choose Task Manager ⇒ File ⇒ New Task (Run) to open the Create New Task dialog box, type **explorer.exe**, and click OK to reload the desktop copy of `explorer.exe`.



TIP

To quickly open Windows Explorer, right-click This PC or Computer and choose Explore from the shortcut menu; while with Windows 10 you can Right-click on Start and choose File Explorer. This Explore option shows up in the contextual menu for any folder. By default, Explore is not in the context menu of Windows 7. An even faster way to open Explorer: Press the Windows key + E.

## *Command line*

The last way to get around on your computer is the oldest of the methods: the command line. While this may look like an old MS-DOS prompt, it is not. When you're dealing with Windows, you are running the 32-bit or 64-bit command-line application. This application can execute any command found on the system, but is most often used for commands without a Windows GUI component. Microsoft has command line tools available to perform most system management tasks from the command line, which is useful when troubleshooting or when creating scripts or batch files to perform tasks.

You access the command line in Windows 7 by choosing Start ⇒ All Programs ⇒ Accessories ⇒ Command Prompt, or with Windows 8.1 and Windows 10, by right-clicking the Start Menu and choosing Command Prompt. If you right-click it, you have the option of running it as the Administrator. Windows 7 and Windows 8.1 allow you to hold Shift while right-clicking a folder and choose Open Command Window Here instead of having to navigate to the path from a command prompt.



TECHNICAL  
STUFF

The latest versions of Windows 10 have replaced the links to Command Prompt and Command Prompt (Admin) when right-clicking Start with the newer Windows PowerShell and Windows PowerShell (Admin), since many administrators now prefer the option to run PowerShell commands over other traditional command-line tools. The PowerShell prompt can run traditional command-line tools, or you can run `cmd.exe` to get to the traditional Command Prompt (all from within the initial PowerShell window).

## *Using Tools and Configuration Utilities*

A computer's configuration is very important for both cosmetic and functional reasons. In the following sections, you get a good look at the tools that you use to manage your system configuration.

### *Control panel applets*

Most settings for your computer are stored in the Registry, but the Registry is a place where if you make an error while making changes, it can require that you re-install your OS. To make your actions less prone to major errors, Microsoft created the Control Panel. The Control Panel contains applets that allow you to change many system settings without requiring you to make direct changes to the Registry. Control panel applets are the recommended method of changing most of your system

settings. [Table 2-3](#) provides a summary of each Control Panel applet and identifies on which OS(es) you'll find them.

**TABLE 2-3 Control Panel Applets**

<b><i>Control Panel Applet</i></b>	<b><i>Description</i></b>
Administrative Tools	Opens a folder that contains the Administrative Tools for Windows. These tools allow you to configure, manage, and control your Windows computer.
Date and Time	Changes the system date, time, and time zone.
Device Manager	Views and changes settings for hardware and driver software.
Ease of Access Center	Changes settings for accessibility features for users with physical limitations.
Folder Options	Changes default folder options. These options are also available through the Windows Explorer Tools ⇒ Folder Options command.
Fonts	Displays a list of fonts installed on your computer, allows you to see what the fonts look like, and allows you to delete fonts from or copy fonts into the folder.
Internet Options	Configures Internet options and connection settings; clears your Temporary Internet Files and History folders.
Keyboard	Changes the sensitivity settings for your keyboard and the layout for your keyboard.
Mail	Configures the mail system for the computer.
Mouse	Configures the orientation, motion, and double-click settings for your mouse.
Network and Sharing Center	Configures connections to your network or other networks.
Program and Features	Allows you to start the installation of programs, displays a list of installed programs that can be removed, and allows you to add or remove optional OS components (such as games).
Personalization	Configures display options. This includes video card settings, screen resolution, color depth (number of colors), and color scheme.
Phone and Modem	Configures dialing rules and modem settings.
Power Options	Configures power management settings for your computer.



<b>Control Panel Applet</b>	<b>Description</b>
Devices and Printers	Adds, removes, or configures printer settings and queues.
Region Language Region and Language (Windows 7)	Configures the OS to support different currency, numeric, date, and time settings for specific countries; inputs and displays languages.
Scanners and Cameras (Windows 7)	Configures installed scanners and cameras. For Windows 8.1, this is found in Devices and Printers.
Scheduled Tasks (Windows 7)	Adds, modifies, or deletes scheduled tasks.
Security Center (Windows 7) Action Center (Windows 8.1) Security and Maintenance (Windows 10)	Configures and reviews security settings for the computer, including antivirus, Windows Firewall, and automatic updates.
Sound	Sets sounds for system events, such as “window open” or “new mail”; configures audio or multimedia hardware.
Speech Recognition	Changes settings for text-to-speech systems or for voice recognition.
System	Configures advanced system settings for hardware and performance. These settings cover hardware profiles, found in Book 6, <a href="#">Chapter 1</a> ; remote settings; and system protection, found in Book 7, <a href="#">Chapter 3</a> .
Taskbar and Navigation (Windows 8.1 and Windows 10)	Configures settings for how items are displayed in the Taskbar and on the Start screen.
Taskbar and Start Menu (Windows Vista and Windows 7)	Configures settings for items displayed in the Taskbar and the Start menu.
Troubleshooting	Common interface for launching a number of troubleshooting wizards to fix common Windows problems.

<b>Control Panel Applet</b>	<b>Description</b>
User Accounts	Configures user profiles and user settings.
Windows Defender	Offers protection against malware, Trojans, and unwanted software.
Windows Firewall	
Windows Defender Firewall (Windows 10)	Contains configuration settings for the Windows Firewall.
Windows Update	Configures the Automatic Update service on Windows and allows you to choose how and when your updates are installed.

All versions of Windows support several power options:

- » **Power plans:** Power plans are preset configuration options for power settings. The plans' names and settings vary between versions of Windows. Power plans allow you to quickly switch between power configurations.
- » **Sleep/Suspend/Standby:** Sleep is a low-power configuration that powers down most of the components of the computer, but leaves some power running through the system memory. When the computer is activated again, all devices are powered back up and the system resumes normal operations. When the system is in Sleep mode, if power is lost, the data in memory is lost.  
 Windows supports a setting called Hybrid Sleep, which puts the computer into Sleep mode and then writes memory data to the hard drive, in the same way as if it were preparing to hibernate, so that if power is lost, the contents of memory are still available. In Hybrid Sleep mode, the computer will resume quickly as in normal Sleep mode. Windows 8.1 and newer Windows OSes always use Hybrid Sleep mode as their Sleep mode. Suspend and Standby are terms that are synonymous with Sleep, but different devices or OSes may choose to use the other terms.
- » **Hibernate:** To prevent data loss and reduce power requirements, Hibernate writes the contents of memory to a file on the hard drive

and completely powers the computer off. In this case, power consumption is equal to that of a powered-off computer. When the computer is powered on, if the memory file exists, the memory information is loaded back into memory, and the computer is in the same operational state as when it went into hibernation.

Windows 7 has the following Control Panel applets, which continue in Windows 8.1 and Windows 10:

- » **HomeGroup:** This Control Panel applet allows you to create or join a HomeGroup. A HomeGroup gives Windows 7 a simplified interface to configure sharing of files and resources between computers. Computers must be configured for the Home network location to participate in a HomeGroup.
- » **Action Center:** Windows 7 provides a central location for problem reports, solutions, and key security and maintenance information, and initiates a recovery to an earlier point of time.
- » **Sync Center:** This is a central location to monitor and resolve issues with sync activities when using the Offline Files feature. Offline files work with network locations, and copies files to your computer to work on when you are no longer connected to the network. When you return to the network, those changes are synchronized back to the network.
- » **RemoteApp and Desktop Connections:** Windows Server 2008 and Windows Server 2008 R2, through the improved Remote Desktop Services, allow the publishing of remote desktop sessions as well as single applications. This Control Panel applet is a client-side connection manager for these remote applications and sessions. This allows the management of these remote services to be centralized in a single location.

## *Microsoft Management Console*

One common complaint about earlier versions of Windows was that you had to use a different management tool for every task. For example, Windows used to have separate tools for managing every aspect of the

server or OS, from managing users or computers in a network domain *and* locally on the computer, tools for managing performance, and tools for managing disks and disk partitions. With Windows 2000, Microsoft took steps to consolidate these disparate tools with the Microsoft Management Console (MMC), and although it has been upgraded, the MMC remains the main management interface for all newer versions of Windows.

The MMC is a framework into which other tools — *snap-ins* — can be loaded. All items that you see in your Administrative Tools folder represent MMC sessions configured with preset snap-ins. To see the raw interface, run `mmc.exe` from the Run command or from the command line.

## ***Taskbar and notification area***

To help you keep an eye on programs running on your computer and to allow you to switch quickly between running programs, Microsoft created the Taskbar. Its default location is at the bottom of the desktop, but it is movable. The left end holds the Start menu, and the other end holds the notification area, which was formerly called the system tray, or Systray. The space between holds tiles representing running applications.

Right-click an empty area of the Taskbar and choose Properties or Taskbar settings to modify settings for the Taskbar and the notification area, such as auto-hiding the Taskbar, displaying the Quick Launch toolbar, grouping buttons, showing the clock, and hiding inactive icons.

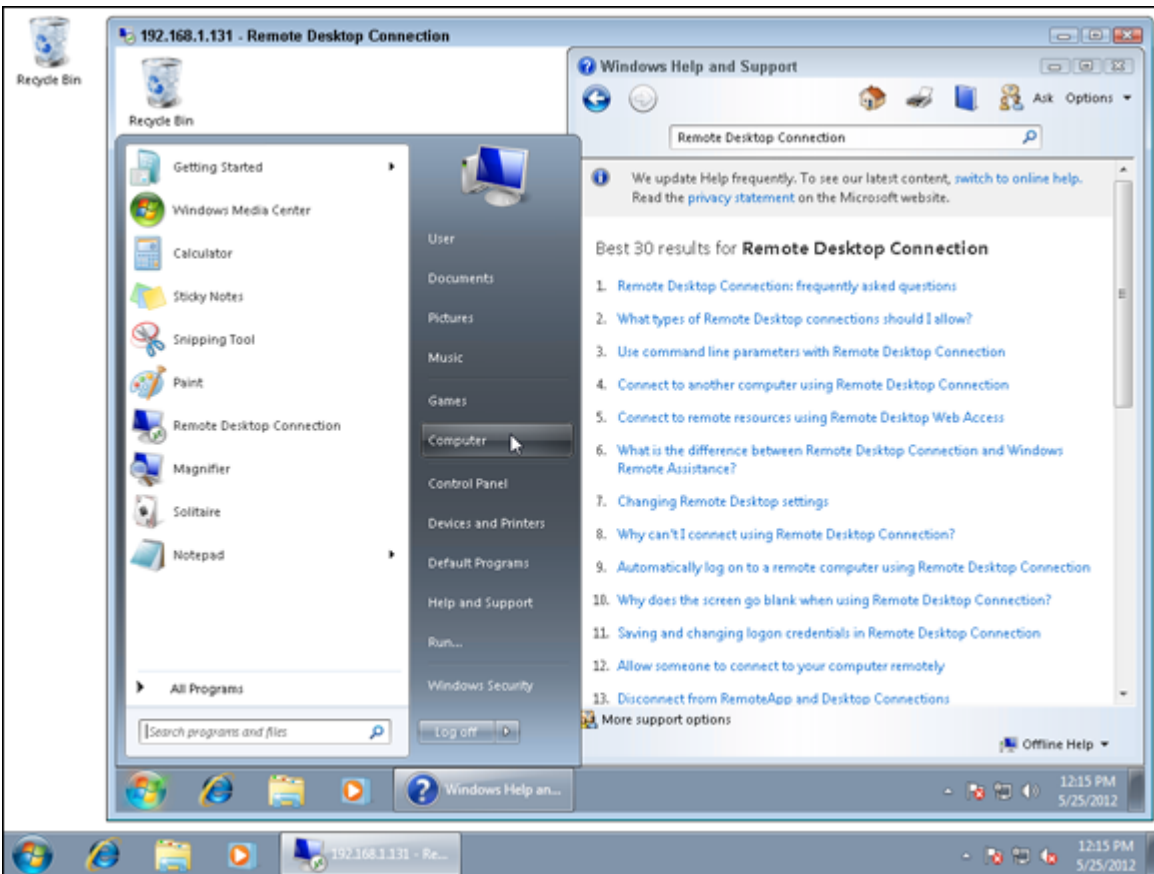
## ***Start menu/Start screen***

If all the items on your desktop were missing, you would still be able to accomplish all that you need to do via the Start menu. Windows 7 streamlined the Start menus, providing an integrated Run/Search command and removing “Start” from the menu name (displaying only the Windows logo). With the variety of Start menu customizations that are available to you, you can still make the Windows 7 Start menu operate like older versions. Windows 8 further enhanced the experience by delivering the Start experience as an entire screen. For people missing the Start button, Microsoft reintroduced it in Windows 8.1, although still linking it to the Start screen, and Windows 10 reintroduced a greatly enhanced Start menu.

The Start menu, like its name suggests, can be used to start most applications on your computer. Contrary to its name, you can also use it to shut down your computer.

## ***Remote Desktop Connection***

There are a number of tasks that you can perform on a remote computer, such as modifying files, changing printer settings, or editing the registry; but there are times that you want to launch and run applications on that computer, and it is at these times you would use Remote Desktop Connection to connect across a network to another computer and remotely take over the desktop or console. See [Figure 2-6](#). The technology in use is the Remote Desktop Protocol (RDP) from Microsoft, which defines how to send key strokes and mouse movements across a network from one computer to another computer, and how to have what is displayed on the screen of a computer sent to another computer. Using these mechanisms, you can remotely use another computer on your network, just as if you were sitting in front of that computer.



**FIGURE 2-6:** A Remote Desktop Connection to another computer on the network.

From a computer running Remote Desktop Connection, you can connect to a virtual desktop on a server running Windows Server, which can support hundreds of remote users simultaneously. Or, you can connect to the desktop of a Windows Desktop computer (not Home or Core editions) computer. In either case, you can run applications on the remote computer as if you were sitting at the computer. Your computer passes mouse movements and keystrokes up the remote computer, and you see virtual screen shots of what is happening on the remote computer screen. **Note:** These are virtual screen shots and not really what is happening on the screen; what you are seeing does not appear on the remote computer screen.

You can find Remote Desktop Connection in the Start menu under All Programs ⇒ Accessories ⇒ Communications, you can launch it from the Run command by typing **mstsc.exe**, or you can choose Start, type **Remote**, and select Remote Desktop Connection.



**REMEMBER** Remote Desktop Connection, through RDP, is a great tool for remotely troubleshooting a variety of problems because it can give you control of a computer on a remote network as if you were sitting right in front of it.

To configure access to your computer from a remote computer, either by a Remote Desktop connection or a Remote Assistance connection, you will use the Remote Settings tab of the System Control Panel applet. To open these settings in Windows 7, choose Start, right-click Computer, choose Properties, and choose Remote Settings. This dialog box allows you to have Remote Assistance sessions, as well as allows the capability to have Remote Desktop session connections to your computer. The Remote Desktop session can also be restricted to the newer and more secure version of the Remote Desktop Connection client software.

## *Remote Assistance*

*Remote Assistance* allows you to ask for or provide help to another person using a distant computer by watching what that user is doing, or by taking control of that computer and having the user watch you.

Remote Assistance uses RDP just like Remote Desktop Connection, but the implementation is very different. As a CompTIA A+ Certified Professional, you will often be asked to help a remote user perform a series of tasks. Many users just need a bit of extra guidance to complete a task, or have a question about something onscreen. After being involved in many telephone conversions with remote users, I can honestly say that a picture is worth a thousand words — sometimes even two thousand. Having the user show you exactly what is happening — or being able to show the user exactly what to do — can save a great deal of time.

Here's how Remote Assistance works:

1. A user who needs help goes to Help and Support in the Start menu and opens the Help and Support Center. (The remote help is here as well.) On a Windows 8.1 or Windows 10 computer, click the Start button

and type **Invite**, then select the link in the search panel for Invite someone to connect to your PC and help you, or offer to help someone else.

2. With Windows 7, click More Support Options to see a link for Windows Remote Assistance, for Windows 8.1 or Windows 10, Step 1 brings you to this point. When the user chooses this and invites you to help, the user has the option of sending an invitation through Windows Messenger or email, or by saving the invitation to a file. Windows 7 adds a key-based Easy Connect, where you simply need to provide the helper with your key.

Regardless of the send-message method used, an invitation file is generated, and this invitation is key to the Remote Assistance system.

3. When the tech opens the invitation, he can open the Remote Assistance application and connect to a user's computer via RDP.

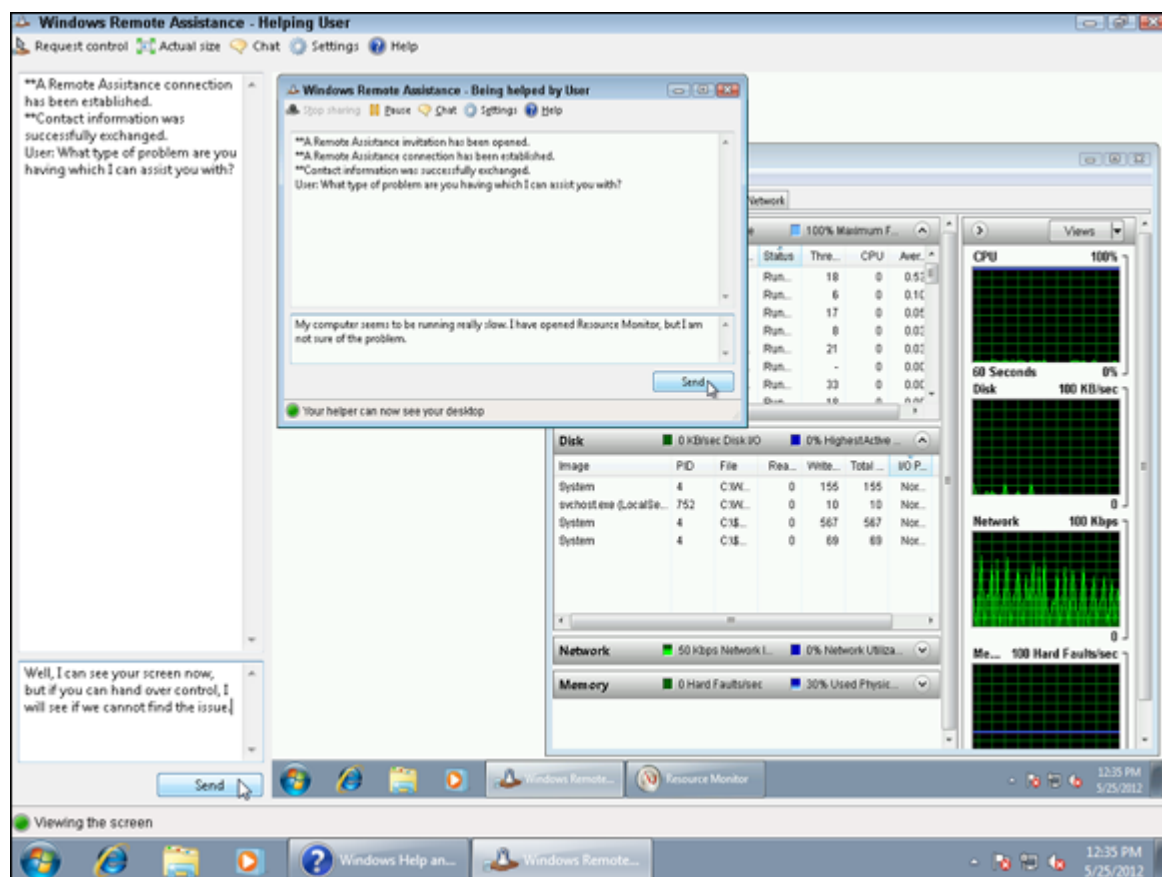


FOR THE  
EXAM

Remote Assistance requests are always initiated by the person requesting help.

The Remote Assistance application also provides a chat section as well as a section where you can see and/or control the remote system, as shown in [Figure 2-7](#). Unlike Remote Desktop Connection, with Remote Assistance, both the local and remote user can see what is going on with the problem computer and can communicate with a built-in Chat application.





**FIGURE 2-7:** The Remote Assistance process can be a boon for many help desk personnel.

## Display settings

Three display settings are covered in the CompTIA A+ exam objectives. These include resolution, refresh rate, and color depth, which will be covered in this section.

Your monitor and video card are capable of a wide range of possible resolutions. *Resolution* refers to the dots or pixels that make up the image that appears on the screen. The smaller the dots, the smoother the image (think of a diagonal line that shows steps at low resolutions). Increasing the display resolution will make the image and icons appear smaller, since the number of dots or pixels that make up the height and width of the icons remains the same, but the size of the dots or pixels is smaller. Although the size of the icons on the screen are smaller, the number of icons you can fit on your screen goes up, so using a higher resolution may give you a clearer image but the size of the items will be reduced.

Screen resolution, especially on laptops, has reached an extremely high level. My current laptop supports a 2560 x 1440 resolution! However, that resolution leaves everything on the screen too small for my old eyes. A tradeoff between resolution and icon size was introduced with Windows 10 in the form of scaling of text and layout. Rather than using a resolution like 1920 x 1080, I can use 2560 x 1440, and then scale the objects by 150 or 200 percent to make the objects appear larger. What does that give me over the lower resolution? I should see smoother images, especially when diagonal lines are concerned.

Image quality has also affected screen refresh rate. *Refresh rate* refers to how many times per second the image on the screen is replaced. On old CRT (Cathode Ray Tube) monitors, an electron gun moved from the top of the screen to the bottom, row by row, lighting up the coating on the back of the monitor's glass. This process was completed over and over again at a consistent speed. Refresh rates are measured in hertz (Hz), which is the number of cycles per second that are completed. The human eye will typically not see any screen flicker at 60 Hz. A rate of 75 Hz can ease eye strain, while 48 Hz can increase it. While today's LCD and LED monitors no longer have an electron gun, they still refresh the image on the screen at specific refresh rates.

Finally, *color depth* refers to the number of distinct colors that can be displayed on the monitor. Color depth is measured traditionally using bits, which represent the number of combinations. An 8-bit number is  $2^8$ , which allows for 256 combinations, while a 32-bit number is  $2^{32}$ , which allows for over 4 billion combinations or colors.

## *Locating Major Files*

File structure and path knowledge is important when using a computer. This section looks at these from a Windows perspective. Many types of files are stored on your Windows computer, and most of these files have standard locations where you can expect to find them. This section looks at the major types of files.

### *User files*

All user-related files have been placed in the `C:\Users` directory, with each user having a folder in that directory. This location holds all files related to or that are personal to that user. This user-specific folder is called the *user profile*, and it includes the following folders (some of which are hidden by default):

- » Desktop
- » Application Data
- » Temporary Files
- » Documents
- » Start Menu

## *System files*

In addition to a number of user useful programs, the Windows OS has certain files required to make the computer operate. The files that are required to make the computer operate are found primarily in the Windows directory. Without these files, the OS would not function. For several generations of Windows, these files have been stored in the folder named `C:\Windows`. Two main sub-directories, named `System` and `System32`, hold critical files for the OS, such as DLLs. 64-bit computers have an additional folder, called `SysWow64`, to hold DLLs and OS files. These sets of system files allow 32-bit Windows to run both 32-bit and 16-bit applications, while on 64-bit Windows, you are able to run 64-bit and 32-bit applications, allowing for some level of backward compatibility.

## *Fonts*

Each font or typeface in use in the OS has its information stored in a file in `C:\Windows\Fonts`. There is one file for each version of each typeface. Font files typically have one of two file extensions: `.ttf` or `.fon`.

## *Temporary files*

Temporary files are stored separately for each user within his or her user profile directory. This allows for security to be placed on each user's temporary files, allowing these temporary files to be kept private and any sensitive data to be kept secure.

## *Program files*

As I mention in the preceding section on System files, some files that ship as part of the OS are critical to the functioning of the OS, but other files that ship as part of the OS are not. For example, `Wordpad.exe` and `MSHearts.exe` are part of the OS (and are useful and fun), but the OS would continue to function without issue if these files were missing. The majority of these noncritical files are stored in the Program files directory, which is `C:\Program Files`, but if you are using a 64-bit version of Windows, you will find these files in either `C:\Program Files` or `C:\Program Files (x86)`, depending on whether the application is 32-bit or 64-bit.

## *Offline files and folders*

When accessing files on a shared folder of another computer over a network, Windows can sync these files automatically to your hard drive. When this happens, the files are put into a folder, but you can still refer to them using their original path, such as `\\<Server>\<Share>\<Synced File>`. These files are stored in a cache, which has a finite size. As total storage reaches the limit of the cache, the oldest nonchanging files are flushed to make room for new files.

# *Examining Windows Features*

You will find many new features and functions with Windows 7, Windows 8.1, and now Windows 10. The following sections introduce you to some of the features that are most important.

## *Aero Desktop*

Windows Vista introduced the world to the Aero Desktop, which allows visual effects such as animations, transparent windows, custom tints, and

thumbnail previews, Aero Snap, to list just a few. Most of these items continue with the current versions of Windows.

## ***Credential Manager***

When you access a shared folder outside of your domain or with alternate credentials, or if you are on a website and provide a username and password, Windows may ask if you want to save those credentials. This is done with the Credential Manager, and those credentials can be accessed through the Control Panel applet of the same name.

Credential Manager allows you see information related to those credentials, which includes the resource you can access, the username, the password, as well as other pertinent information for that resource. Credentials for web resources are separate from Windows resources. For Windows resources, you can pre-add credentials you know you will be needing in the future. You also are able to selectively remove any credentials you no longer want or need saved.

## ***User Account Control***

To increase security and reduce the risk of accidental changes happening on your computer, Microsoft has introduced User Account Control (UAC). Many of the changes you make on your computer can have serious implications to the overall system stability. When UAC is enabled, all major system changes require acknowledgment before committing to changes. When configuration applications are launched, or when changes are detected, UAC presents a confirmation dialog box. To find out more about UAC, review [Chapter 2](#) of Book 9.

## ***BitLocker Drive Encryption***

Windows 7 Ultimate and Enterprise editions include BitLocker Drive Encryption, which is a low-level hard drive encryption component that can encrypt the entire contents of a disk volume. After you enable this feature, all files that you save to your hard drive volume are automatically encrypted. While you can access these files without additional effort, others will need to enter your password to gain access to the files. Not

only are you able to encrypt volumes on your internal drive, but BitLocker-To-Go also allows you to encrypt a removable flash drive.

## ***ReadyBoost***

The ReadyBoost feature is an example of a little going a long way. On a computer with a standard hard drive, there is a penalty every time you read data from the drive, due to the rotational nature of the drive, which means the heads of the drive need to wait for the data that you are looking for to be present under the drive heads. This is called *seek time*. SSD (Solid State Drives) do not have this problem as data is stored in flash memory rather than on disk platters. Drive manufacturers use small amounts of fast cache memory to offset the issue through a system of read-ahead caching, where the drive guesses what data you want next by using a formula or algorithm.

ReadyBoost takes read-ahead caching a step further by allowing you to attach flash media to your computer (in the form of USB flash drives, SD cards, or CompactFlash), and then using that media as additional fast cache memory. By increasing the amount of cache you have available, Windows 7 increases the effectiveness of read-ahead caching, while Windows 10 allows you to use multiple devices. If you are using SSDs, you will not get a benefit from this caching, as those drives are already as fast as you can get, but for your 5400 rpm and 7200 rpm HDDs, you will see a large benefit from ReadyBoost.

To enable or disable ReadyBoost on your flash media, use the Ready Boost tab from the media Properties dialog. To open the Properties dialog, right-click the drive in Computer and select Properties.

## ***Volume Shadow Copy Service (VSS)***

Shadow Copy is a feature introduced in Windows XP and is now referred to as the Volume Shadow Copy Service (VSS). VSS is an application programming interface (API) that supports copying data at a low level of the file system. It offers the benefit of being able to copy files that are open and being accessed, which it does by temporarily placing the files in a locked state. The magic of VSS is how it instantaneously locks the drive, but then creates a copy of any files to which a write or commit data

operation is issued. When the write operation is requested for a file, VSS then creates a copy of the file in the VSS cache before actually performing the write operation to the file on the disk. This action is called *copy on write*.

In addition to the core API, VSS copies of drives can be scheduled, which causes any new file writes to be committed to a new copy of the files. This is managed on the fly at the file system level.

## ***System Restore and System Protection***

Windows client operating systems have a system of restore points that are created automatically or manually to manage system files, the user's files are not touched in this process. Automatic restore points are created when major events happen, such as application installations, driver installations, or other similar events. Users can manually trigger the creation of a restore point by using the System Protection tab of the Advanced System Settings of the System Control Panel.

This restore point process is tied to VSS, which is the service that is used to create the backup files. The process of reverting to a restore point is called System Restore. Full coverage of recovery points and the System Restore process is found in Book 7, [Chapter 3](#).

## ***Compatibility Mode***

With each new version of Windows that arrives on the market, some applications do not operate in the new OS. To assist with getting these applications to work, Microsoft offers a series of tweaks that can be enabled for the application through its Properties dialog box. These options have been growing since Windows 7.

*Compatibility Mode*, as the name suggests, is about making the OS more compatible with the application. As the Windows OS evolves, changes are made in how it manages the display resolutions and with many internal system processes. These changes sometimes cause older software to not run quite correctly — like changes in car models from one year to another that may cause old accessories to not fit properly in the newer models. The best solution is to upgrade to the latest version of the software, but when that is not an option, you can use Compatibility Mode

to try to continue do things in the older version of the software that does not work with the newer OS. More on Compatibility Mode can be found in Book 6, [Chapter 2](#).

## *Windows Easy Transfer*

Upgrading to a new computer can be a large pain. Windows has the File and Settings Transfer Wizard, which has been dramatically improved with each release of Windows. The new version makes it easy for you to transfer your files, email, pictures, and settings from your old computer to your new computer. Easy Transfer adds a friendly front end to the User State Migration Tool (USMT), which is used in large enterprises to migrate user settings. Unfortunately, Easy Transfer was removed from Windows with the release of Windows 10.

## *Pinning*

When you have programs you run frequently, it can become a pain to constantly locate these applications in the nested Start menu or Start screen. Many people used to take the applications they use on a regular basis and put shortcuts on the desktop, but to access them users still had to minimize the open windows to get to the desktop. Windows 7 maintains a dynamic list of recently used applications in the Start menu, but there are a limited number of items that are kept in the list. To solve this, Windows enables you to pin items to the Start menu so that they are always available right on top of the menu.

Windows also gives you the added option to pin application shortcuts to the Taskbar, making them even more easily available to you — no window minimizing at all. If you are using Windows Explorer, then you have an option to pin folders to the Quick Access area of the Explorer window.

## *Event Viewer*

Many components of the Windows OS log information when certain events happen. The events may be informational, warnings, or critical items. Windows logs them to one of three logs: System, Security, or Application. These logs can be viewed with the Event Viewer, which is



found in the Administrative Tools folder and is discussed in depth in Book 6, [Chapter 4](#).

## *Administrative tools*

All versions of Windows based on the NT base have included Administrative Tools, which is a folder (now located in the Control Panel folder) that contains the main tools for administrating a Windows computer. On Windows 10, you will also find Administrative Tools in the Start Menu under Windows Administrative Tools. In addition to the Event Viewer, many administrative tools are covered throughout this book. These tools include Component Services, Computer Management, ODBC Data Sources, Event Viewer, iSCSI Initiator, Local Security Policy, Performance Monitor, Print Management, Services, System Configuration, Task Scheduler, Windows Firewall, and Windows PowerShell.

## *Control Panel views*

With every generation of the Windows OS, the number of Control Panel items grows. To deal with this sprawl, Microsoft created Category View for the Control Panel. This view takes all the icons and places them within eight to ten categories (depending on the OS). Windows 7 and Windows 8.1 use these categories by default: System and Security; Network and Internet; Hardware and Sound; Programs; User Account and Family Safety; Appearance and Personalization; Clock, Language, and Region; and Ease of Access. All the other Control Panel applets are placed into one of these categories.

While the Category view was designed to make Windows easier to use and navigate, users familiar with the old, flat folder structure can be at a loss to find what they are looking for. Because of this, you will find an option in Windows Vista to switch to Classic View, which simply shows all the Control Panel applets by name. In Windows 7 and Windows 8.1, you find a small menu giving you the options of viewing by Category, Large Icons, or Small Icons (where the icon views are equivalent to Classic View). Old habits die hard sometimes.

Windows 8.1 and Windows 10 also make use of the Settings application, where you will find many items you would have found in Control Panel.

While the Control Panel applets may still exist, the move is underway to move all this functionality into Settings.

## *Virtualization Platforms*

*Virtualization* refers to the creation of one or more virtual computers to run software existing on the physical computer. The computer that plays host to these virtual computers runs a piece of software called a hypervisor. The hypervisor manages the virtual computer, which, like a physical computer, is made up of a processor, RAM, hard drive, and other peripherals, but limits exist as to what hardware can be virtualized. The hypervisor starts the virtual machine and allows the installation of an OS onto the virtual computer.

You may be asking “Why would I want this?” Virtual machines offer many benefits. In the past, if I wanted to set up a lab to conduct a test of Microsoft Exchange replication, web services failover, or WSUS (Windows Server Update Services), then I might need three to six computers available to me, along with some networking hardware, and hours to set up the hardware and operating systems. With virtual machines, assuming I have enough RAM and processing power, I can have all these virtual machines running on a single desktop or laptop computer, including a software-based switch or router. My base server hard drive can be set up and used as a base for all my other servers, greatly reducing the OS installation and setup time. That assists me with server work, while in the developer or desktop management roles, I can test my software on Windows 7, Windows 8.1, and Windows 10 virtual computers without needing different computers to test with. In addition, I can test software installations or migrating user data between computers, and then roll that entire computer back to a state before I tested the migration, allowing me to do it again.

For the security and enterprise software managers, having a farm of virtual machines in a safe data center allows remote users to connect to and control those computers, leaving the applications and data in the data center, and no actual data coming out to that remote computer. Bring Your Own Device (BYOD) initiatives allow those users to connect to the

virtual machine farm to run their applications, which means security can focus on the devices it controls and leave the management of user devices with the users (with some requirements). In the data center, instead of providing separate servers to each team that needs one, a virtual server for each team can be created on a larger physical server, allowing for better resource sharing, utilization, and management. Virtual machines open up a wide range of possibilities of uses and functions, and can change the way we manage our desktops and servers.

Many modern processors and motherboard BIOS/UEFI configurations now have virtualization options that must be enabled if you are going to run a hypervisor on them. In some cases, your software will not install if these options are not enabled, and when this happens, it will usually tell you in the error message that the BIOS settings must be enabled to permit installation or operation.

From a management perspective, each of these virtual computers is a full-fledged computer running an OS. But in actuality, all the running virtual computers are sharing the resources of the host computer running the hypervisor. Some common desktop hypervisors include the following:

- » Microsoft Virtual PC
- » Microsoft Hyper-V
- » VMware Workstation
- » VMware Fusion
- » Oracle VM VirtualBox
- » Parallels Workstation
- » Parallels Desktop for Mac

When dealing with the large scale virtualization of your servers, your company data center will be filled with powerful servers, virtualizing other servers. Some common datacenter hypervisors include:

- » VMware ESX Server (part of vCenter suite)
- » Microsoft Hyper-V

## » Citrix XenServer

Whether on the desktop or the server, the main purpose for using virtual machines is for resource management or simulation of networks. When you run a virtual machine on a virtual server you call the virtual machine the *guest*, while the server is referred to as the *host*. When you virtualize computers, you gain the following advantages:

- » The hardware is separated from the OS, making server replacements easier to achieve.
- » Hardware is utilized better. Servers often have large periods of idle time, and by running more than one virtual server on that hardware, you are able to bring the utilization of the hardware from under 10 percent in some cases, to greater than 90 percent.
- » Greater uptime or availability as virtual machines can be moved between servers with little or no impact to operations, allowing for hypervisor or hardware maintenance.
- » You can duplicate the structure of a larger networks and a large number of servers.
- » You can set up Lab, Development, and Pre-Production environments for testing and development.

When planning a virtual server environment, there are a few things to remember:

- » **Hypervisor requirements:** These are the requirements for installing and running the hypervisor. This will include requirements for the storage controller and devices, as well as the requirements for the network controller. In most cases, the requirements for running the hypervisor are quite low.
- » **Resource requirements:** Unlike the requirements for the emulator, the overall resource requirements will be much higher. If you plan to virtualize 20 of your production servers on a single virtualization server, you will require a high level of resources. The actual amount of resources will depend on how much are actually in use. VMware

has a sizing tool named Capacity Planner that monitors your servers for a period of time and calculates the size of your virtual servers hosting them based on the processor, disk, network, and memory resources actually in use.

» **Emulation requirements and Virtual NIC:** When working with connecting virtual or physical hardware to your virtual machine, you have some choices, and these will be dependent on the OS you are installing on your virtual machine, as well as the hypervisor you have chosen to use. Your choices are emulated hardware, para-virtualized hardware, or passthrough connections to the hardware. When looking at network cards in VMware server, you have three choices:

- *E1000e*: An emulated network card that appears to the OS as an Intel EtherExpress Gigabit network adapter. This is a common network adapter and VMware expects that almost every OS will include a driver for it. This makes this network interface very easy to include in any OS. Because it is an emulated interface, you can expect that there will be performance loss as data and signals from the virtual network adapter need to be translated to a physical network adapter. This process also means that it does not matter what the underlying network adapter is — the OS will always see an Intel network adapter.
- *SR-IOV passthrough*: The passthrough adapter makes a direct connection from the virtual machine to a physical network card. This removes all layers between the virtual machine and the network, allowing maximum performance. One issue is the mobility of the virtual machine and the need to change the network adapter drivers when moving to a server with a different network adapter.
- *VMXNET 3*: The VMXNNET 3 is a para-virtual adapter. This requires special drivers or support in the OS, but also still provides an abstraction layer between the virtual machine and the physical hardware on the hosting server. The abstraction layer allows the machine to be moved to a server with different

hardware and still operate, but the customized drivers allow for better performance and advanced features, which may not be provided by the emulated Intel network adapter.

- » **Security requirements:** When you grant a user access to your virtual host, you are potentially giving that user access to all the guest machines on that server. Special care must be used to ensure that users only have access to the required guest machines.
- » **Network requirements:** When working with a virtual server, some thought should be given to the amount of data guests will generate. If each guest can generate 500 Mbps of data, and you plan to run ten guests on the host, you would need sufficient network resources to accommodate 5 Gbps of network activity. With guest machines acting as virtual routers and firewalls, you are able to create an entire network of servers on a single virtual host, including VLAN segments and all of the resources you would expect on a network.

By using virtual computers, you are able to create an entire test lab of servers and workstations on a single computer. While this is possible, remember that each virtual computer you start up is going to attempt to use resources of the host to perform operations. So if I have a computer with 8GB of RAM and I start up three virtual computers, each using all of an allocated 2GB of RAM, I only have 2GB of RAM for operations on my computer. Many hypervisors allow me to oversubscribe, so I could start up six computers, each with 2GB of RAM, on my 8GB computer. But as you can guess, if they all try to use all their memory, my host computer will start paging a substantial amount of data to the hard drive, slowing all the virtual computers. This issue of resources is not only true about RAM but also CPU cycles, disk access, and network access. Oversubscribing is possible, but you should avoid it if you want good performance.

## *Virtual Desktops*

It has been many years since Citrix and Microsoft released terminal services. These services, however, have a few drawbacks. One drawback

is that these services require that many users are logged onto a single machine, all running applications in the same environment. This configuration may work well for many applications, but as soon as you encounter an application that cannot be run on a machine more than once, you have hit a wall. The solution to this issue is to create a separate virtual machine on a virtual server, like the ones mentioned in the previous section, and allow users to connect directly to those machines. Since each user receives his or her own virtual machine, there is no issue with two users running the same application on the same machine at the same time, as there is only one use on each machine at the time.

Although I can manually create a large number of virtual machines for users on the virtual server, this can quickly become a cumbersome process. Thus, the major virtualization providers have come up with solutions to make this process streamlined, as well as optimize storage management and security through the use of clones and wiping machines between users. The name given to this new technology and processes is *virtual desktops*. Users are given a single desktop experience with these remote virtual machines.

When deciding to use terminal services in an organization, it is normal to also implement thin client technology for users rather than supplying them with full computers. These same thin clients can be used for connecting to their virtual desktops.

The server processing power required to manage virtual desktops exceeds that required to provide services on a terminal server, since there is overhead for the OS on each virtual machine; these increased server resources are offset by the increase security and separation of users.

## *Going to the Cloud*

*Cloud computing* is the practice of using a network of remote servers over the Internet to store and access data rather than a local hard drive. The National Institute of Standards and Technology (NIST) defines cloud computing as a computing model that adheres to the following five principles:

- » **On demand service:** With traditional servers, when users decide they need an additional server, it can take weeks or months to select the new hardware, get approval to purchase it, and get it shipped in, racked, set up, the OS installed, and prepared to host the application that was intended for it. On demand means that once you decide you need another server, you can go to the web portal, and with a few clicks and a short wait, your server is ready for the application to be installed.
- » **Rapid elasticity:** *Elasticity* refers to the ability of the server to expand or contract based on need. For example, if you run a website that sells concert tickets, rapid elasticity is needed on days when new concerts are added for sale. If your web application normally runs one instance and supports 1,000 concurrent sales transactions, it will be overwhelmed when the latest hot concert tickets start selling and 50,000 users try to buy tickets at the same time. With elasticity, you can set a threshold so that when 80 percent of the connections are open, the cloud service will start up one or two more instances of the website. As the total number of connections start to fall as all the tickets are sold, the additional instances of the website will be shut down and destroyed or de-provisioned. You will only pay for the additional instances when they are provisioned and running.
- » **Resource pooling:** With resource pooling, the cloud provider pools resources within its environment, so that several clients are running virtual machines and websites on the same server. Clients are segregated from each other, but they may be running on common servers and using the same storage, network switches, and routers. Resource pooling enables rapid elasticity between clients, such as the concert ticket website that may need to expand resources when the next hot concert comes to town, and the florist, who may need extra resources around Valentine's Day and Mother's Day. Resource pooling is more of a feature that benefits the cloud services provider rather than the consumer of the services.
- » **Measured service:** A measured service is a service that is monitored and measured against a set of standards, which are defined in a



service contract. The information in the measured service is used for resource management, resource planning, and billing.

- » **Metered:** A metered service is a service for which you pay for the amount of service you consume. If you think of your home, this is how you are likely paying for electricity and water. When dealing with cloud solutions, you may be paying per unit of CPU use, the amount of storage you are consuming, or the amount of data you transfer to or from storage locations, or in and out of the cloud service.
- » **Broad network access:** To be a worldwide provider of cloud services, a company needs to provide access to resources and have resources around the world. This is often done by providing data centers in different areas of the country or the world, and by providing network access points in a wider variety of locations.

You will find that all major providers of cloud computing solutions include these five components.

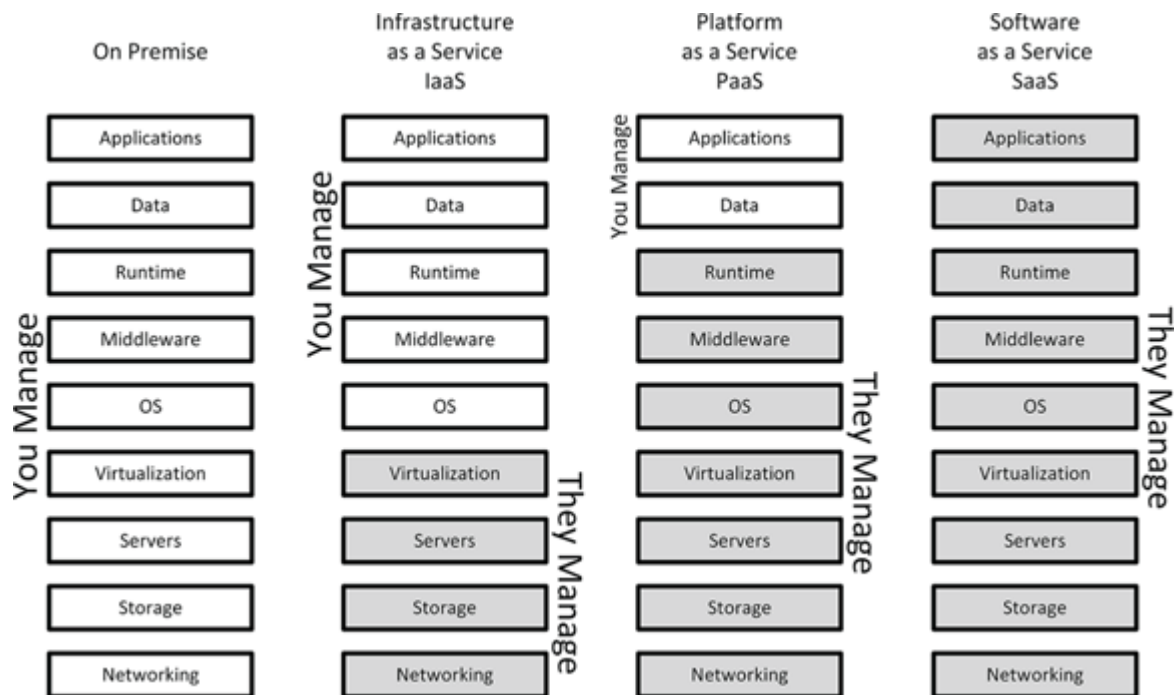
## *Evaluating cloud models*

Take a look at [Figure 2-8](#) and focus on the first column of boxes. This column represents all the layers that make up a server (or group of servers) hosting an application. From the bottom up, resources are broken into three main layers, or categories:

- » **Physical infrastructure:** The physical side of the equation includes switches, network cards, storage or disks, physical servers hosting those components, and a virtualization hypervisor. Many large organizations have made the move from physical servers hosting applications to virtual servers running the actual software. In the end, this whole category refers to the hardware that is sitting in a server rack to run an application.
- » **OS and middleware:** When hosting a traditional piece of software, there are often two layers: one that the client sees and one that contains managing software or business logic. This includes the OS or may start above the OS level. For our purposes today we are going to place the OS in this group. Software runtime components are also

included in this level. An example of this is a SQL database server. If you are an accounting server, all the data and many of the calculating components would be hosted on the SQL server, which the users of the software never deal with directly.

» **Application:** The application layer contains the application and the application data. These are the things that the user of the application would see, be aware of, and know very well.



**FIGURE 2-8:** A comparison of cloud services and management responsibility.

These layers make up most server-based applications in a corporate environment. These applications run such business operations as production scheduling; assembly lines; budgeting, payroll, and enterprise accounting systems; customer relations and tracking systems; sales; and invoicing. These systems are typically run by the internal IT department, and the cost of purchasing and operating the equipment is either absorbed as overhead or charged back to the department using the equipment.

When you set up a method to separate department services onto different virtual servers and provide the departments easy methods of provisioning their own virtual servers, web applications, and other resources, you have created a cloud-like environment — a *private cloud* — inside your own

private network. There is nothing too crazy about a private cloud; in fact, some companies may be providing it without using the name.

## COMMERCIAL PRIVATE CLOUD

Large cloud providers, such as Microsoft and IBM, provide what they call “private cloud offerings,” where they provide an equivalent of their cloud tools that can run on your internal network. IBM calls its product IBM Cloud Private, and it encompasses major components of IBM’s cloud solution tailored to run on your network, server, and storage infrastructure. Microsoft provides a product it calls Azure Stack, which is a subset of the Azure virtualization environment preinstalled on server hardware that can be augmented by your own storage and runs over your network infrastructure. The benefits you have with these private cloud solutions include:

- Configuration methods and tools are the same on your private cloud as you would use with their public cloud solutions.
- Integration with their public cloud solutions, allowing for easy migration of workloads between the public and private cloud offerings.

The *public cloud* by comparison moves the computing infrastructure outside of your private network and to a public cloud service provider, or in some cases to a smaller company that provides the hosting of your virtual infrastructure. (The following section covers the three main public cloud offerings in more detail.)

So you have seen private cloud and will see public cloud; so where does a *hybrid cloud* fit into the picture? If you choose to move only some of your infrastructure and services to a public cloud provider, you are in a hybrid state, with both public and private clouds supporting part of your services. For some organizations, a hybrid cloud is an end state, while for others it is a transition state between private cloud and public cloud.

The final cloud option is a *community cloud*, which refers to a cloud-services solution set up by a group of organizations. Unlike setting up their own private cloud solution, which may be too large for an

organization individually, the cost of the cloud infrastructure is shared among all members of the community. Usually these organizations already have a close working relationship and common security goals or needs, which makes sharing the infrastructure easier.

## WHAT'S WITH INTERNAL AND EXTERNAL CLOUD?

Given the opportunity and the time, especially with new and confusing technology, people will continue to come up with new and creative terms, or merely mix up terms. When working with cloud solutions, you should limit your list to private, public, hybrid, and community clouds. When working with resource types or resource locations, then you can work with internal and external, which makes reference to where these resources are located. *Public cloud* will always be paired with external resource types, while *private cloud* would typically be called internal resources. The only situation that could confuse the issue is if your company sub-contracts data center services to a third party, which could then be considered an external resource, but that could be debated. The answer often comes down to ownership.

So there are no internal and external clouds, only internal and external resources.

When looking at sharing resources, such as setting up multiple virtual servers on a physical server, you will have control over this sharing when working with internal resources. However, you will have little or no control when working with external resources. When working with a cloud provider, you may have high availability options, which can ensure that two specific virtual resources are in separate physical servers, in separate server racks, on separate power supplies, or in separate data centers, or even in separate countries. This helps to ensure that your two servers share no resources whatsoever.

### *Common cloud models*

[Figure 2-8](#) shown earlier illustrates the components that make up any server-based solution, from the network to the servers to the databases to the front-end applications and their data. These components are the same whether you are managing the whole show, or whether you have someone else managing it. But there may come a time when you feel it is easier and

cheaper to get someone else to manage those components. The following sections outline three public cloud offerings.

### *Infrastructure as a Service (IaaS)*

Infrastructure as a Service (IaaS) is a form of cloud computing that uses virtual machines managed by someone else, like Microsoft Azure. This means that you choose a level of virtual machine you would like, and the IaaS provider will provision or create and prepare it for you. Your virtual machine files need to be stored someplace and needs some network connectivity, so prior to choosing your machine, you should create a storage location (a few menu clicks) and set up a virtual network (a few more menu clicks). If you do not set up these items, they will be automatically created for you by your IaaS provider, but there may be some restrictions you do not want.

So in the end, you will have a virtual machine (VM) running on a Microsoft Hyper-V server hosted in a remote Microsoft datacenter. You can now use Remote Desktop Protocol (RDP) to connect to your new server and do whatever you need to have your required software function. Microsoft takes care of the host that is running your VM and relocates the VM to a different host when the current one needs maintenance or needs to be rebooted. It also takes care of your storage and networking needs, so again you have no management responsibility. You are only responsible for what needs to be on the server console, such as patching, defragmenting the disks, and other actions you would take care of at the OS level.

There is a cost for this service, which will vary depending on whom you use for your cloud provider. Microsoft will charge you a little bit for the memory and process cycles you are using when your VM is running, a little bit for the amount of storage you are using, a little bit for any data you transfer out of the server (but not into the server), and a little bit for any licensed software it provides. For example, if you choose a Microsoft SQL server from the catalog of pre-built VMs, you will pay a usage fee for the Windows OS and for the Microsoft SQL server, but if you choose an empty VM and install your own licensed Windows OS and Microsoft SQL server software, your usage costs will be less.

Now I like food, so to put this in food terms, if I am going to make a turkey dinner, I can go buy the turkey, carrots, potatoes, and so on, and bring it all home and cook it. One year my stove stopped working so I brought my ingredients to my sister-in-law's house to use her stove — her infrastructure with my food. After cooking on her infrastructure, I was able to take my meal home and eat at my table. The end result was I still got turkey dinner at Thanksgiving, but I did not have to worry about electricity, repairs to the stove, and eventual replacement of the stove. This is IaaS: the use of someone else's infrastructure to support your server.

IaaS is one area where you will see a lot of Hybrid Cloud implementation, as you are able to create synced copy of your Active Directory user accounts in the cloud, or you may want to create a site-to-site Virtual Private Network (VPN) to your cloud-based servers, making them an extension of your corporate network.

### *Platform as a Service (PaaS)*

Another public cloud offering is Platform as a Service (PaaS). With PaaS, you take this movement of responsibility one step further than IaaS: You give up detailed access to the OS and its management. Now you could create a server using IaaS, install IIS, .Net, a simple database to store user settings, and install your web-based application or service on top of that, but if you are primarily a web-developer or an overworked IT administrator, that takes time and requires ongoing maintenance. PaaS is the solution. When you go to your cloud provider, perhaps Microsoft Azure, you can choose to create an App Service or Cloud Service, both of which are web-based applications. By choosing this option, you have now removed the server administration work from maintaining this application. You no longer need to patch the server, manage the drives, or perform other mundane tasks; you only need to worry about your application. Your costs again vary by the size or power of the server that hosts your web application, but you no longer need to worry about the details of server management.

In terms of my turkey dinner, with PaaS, I choose to buy a prepared and already stuffed turkey and premade salad, potatoes, and vegetables. I

return to my sister-in-law's house to heat the meal, so I still do not have to worry about the infrastructure. In the end, I return to my house to eat and clean my dishes.

### ***Software as a Service (SaaS)***

The third public cloud offering is Software as a Service (SaaS), which takes software and server management, or lack of management, one step further. SaaS is a software licensing and delivery model. With SaaS you are only concerned with what the software can do for you, and not how it does it.

A couple of examples of SaaS in action are using external email through Microsoft Office 365 or Google Apps. In this case, I can still use my email client or a web interface to get my mail. I don't have to worry about Microsoft Exchange servers, managing and patching the server OS, high-availability options, hardware replacement, or anything else involved in managing a Microsoft Exchange server farm. Another example is using a contact management solution through Salesforce, which involves no infrastructure on your end. Simply by filling out a few web pages, you can be running a contact management server completely managed by someone else in the cloud.

To continue the food example, I now choose a nice restaurant and go out for turkey dinner with all the fixings. It is not exactly like the dinner I would cook, but I did not have to buy and prepare the food, buy an oven to cook it in and plates to serve it on, or clean everything up after the fact, and if I do not like the service or food in that restaurant, next time I can always go to the competition down the street.

### ***Examples of cloud services and cloud-based applications***

Two examples of cloud services and SaaS really stand out: off-site email and file synchronization services.

*Off-site email applications* are great examples of SaaS applications. In this field, two companies stand out among the rest: Microsoft (with Office 365 and Outlook online) and Google (with Google Apps and Gmail).

Both of these products allow a user to work with email, create and manage documents, and perform many other tasks, all without having to install an application. All the document and email storage remains in the cloud on servers owned and managed by Microsoft and Google, and users or companies only have to pay a fee to have access to these services. In many cases, the amount of space available for email and document storage far exceeds what users would have been allowed when these services were provided internally.

In both of these cases, Microsoft applications and Google applications, you are able to work with web versions of the applications to read your mail and edit your documents. Both offer stand-alone email applications for all your computing devices, from smartphones to tables to laptops and desktops. When working with your documents, such as letters and spreadsheets, you also have options to work with either the web versions of the applications, or work on offline or stand-alone versions of the applications. These applications may differ between your devices; for example, Microsoft offers a mobile version of its applications for smartphones and tablets, while a more feature rich version may be installed on laptops and desktops.

*Cloud file storage services and synchronization apps* are another popular area, and again we can look at two of the largest: Microsoft OneDrive and Google Drive. In both cases, these services allow users to store any electronic data on their storage servers. In most cases, these files can be fully integrated with office applications and email, and both companies offer a large amount of storage. Being able to store your data in the cloud allows you to access the data from anywhere in the world. To deal with your data when your computer is not connected to the Internet, the solution used by both companies is to use a small agent or program on your computer whose job is to synchronize your data between your computer and your cloud storage.

The synchronization applications for these services are available for all platforms, but both companies typically offer different services when these services are installed on full-fledged computers, like laptops and desktops, instead of smartphones and tablets. Applications for



smartphones and tablets acknowledge that smartphones and tablets are often limited in storage capacity, so the synchronization applications tend to limit the data copied to devices using such methods as only copying data to the device once it has been accessed, and clearing the locally cached data on a more aggressive schedule. Some of these ideas have made it back into the applications for laptops and desktops. For example, Microsoft's OneDrive sync client used to sync all your data; now it can be configured to only sync data and files you have opened and accessed.

## *Virtual Applications*

To wrap up the discussion of virtual technologies, the last stop is virtual applications. Application virtualization is different from cloud-based applications and applications running on virtual machines somewhere in your data center; virtualized applications run locally on your computer and not in some remote location. So what makes these applications virtual, and what are their benefits?

Virtual applications, using a product like Microsoft's AppV, are applications that are run in an isolated memory space, which keeps them separated from other applications running on your computer. This isolation prevents a poorly behaving application from affecting other applications on your system, as well as prevents a malicious program from getting out of this application space or into this application space. It is application isolation.

Another benefit of AppV and many application virtualization solutions is just in time delivery of the application. AppV allows you deploy just shortcuts to an application or to perform a full installation. When installing only the shortcuts, the launching of the application triggers the installation, which then starts in a specific order, where the main executable is installed first, allowing it to launch for the user, while the rest of the supporting files that make up the application install in the background. The term that used to describe this type of application installation process is *streaming*, as the application is streamed to the computer in a specific order to allow the smallest possible delay between the user activating the shortcut and being able to use the application. This

unique installation method does not change the memory isolation that is provided to the application; it only affects:

- » How long it takes to show the user the application is installed, which is only publishing the shortcuts to the application
- » How much space is used on the local drive if the user never launches the application, which is only the space used by the shortcuts
- » How long it takes to activate the application the first time it is launched, which is the time taken to stream or download the main executable and the required core .dll files

## *Getting an A+*

This chapter takes a look at the major functions of a Windows OS. To be prepared for the A+ exams, you should remember the following:

- » The OS is responsible for managing the interface between all hardware components that make up your computer.
- » Virtual memory is composed of physical memory or RAM and space on your hard drive in the form of a paging file.
- » NTFS is the most robust and stable of the available file systems but is compatible with the fewest other OSes.
- » System and application settings are stored in the Registry or in INI files.
- » `explorer.exe` makes up most graphical navigation of your computer and is represented as both My PC and Computer and the desktop.
- » Control Panel applets offer interfaces to many system settings for your computer.
- » Remote access to computers is available through both Remote Desktop Connection and Remote Assistance, both of which rely on the Remote Desktop Protocol (RDP).
- » The difference between cloud services solutions is who is responsible for what pieces of infrastructure.

- » Public and private clouds both make use of common technology solutions such as virtualization. The difference is ownership of the underlying technology and visibility of the technology. In public clouds the technology is hidden from the consumer.
- » Virtualization solutions allow for better utilization of the underlying hardware.

## *Prep Test*

- 1. Phil is using a Windows 7 computer and has run into a problem. He has called you on the phone and has asked for you to open a Remote Assistance connection to his computer to walk him through the solution. What is the first step that you must take?**
  - (A) Open the Remote Desktop Connections program.
  - (B) Ask Phil to choose Help and Support from the Start menu.
  - (C) Ask Phil to run `geninvite.exe` from Start ⇒ Run.
  - (D) Open the Remote Assistance program on your computer, File ⇒ Connect to computer, and choose Phil's computer.
  
- 2. You have been asked to explain virtual memory to an executive in your company. You tell him that virtual memory is composed of which of the following? (Choose all that apply.)**
  - (A) Physical memory
  - (B) Extended memory
  - (C) Hard drive space
  - (D) Compressed memory
  
- 3. Bill is looking to see whether he has Service Pack 1 installed for Windows 7. He went to the System Information Tool located at Start ⇒ All Programs ⇒ Accessories ⇒ System Tools. Is there a quicker way he could have found out this information?**
  - (A) He could have used the Run command to run `systemtool.exe`.

- (B) He could have right-clicked My Computer on the desktop, or from the Start menu, and chosen Properties.
- (C) He could have used the command line tool `ver` from any command prompt.
- (D) There are no other locations in the OS where this information can be displayed.

**4. Your computer has just suffered from a Stop event (also known as the Blue Screen of Death). You are trying to decide what has caused the error. What is the most likely possibility?**

- (A) A multimedia application
- (B) A background application
- (C) A network error
- (D) A system device driver

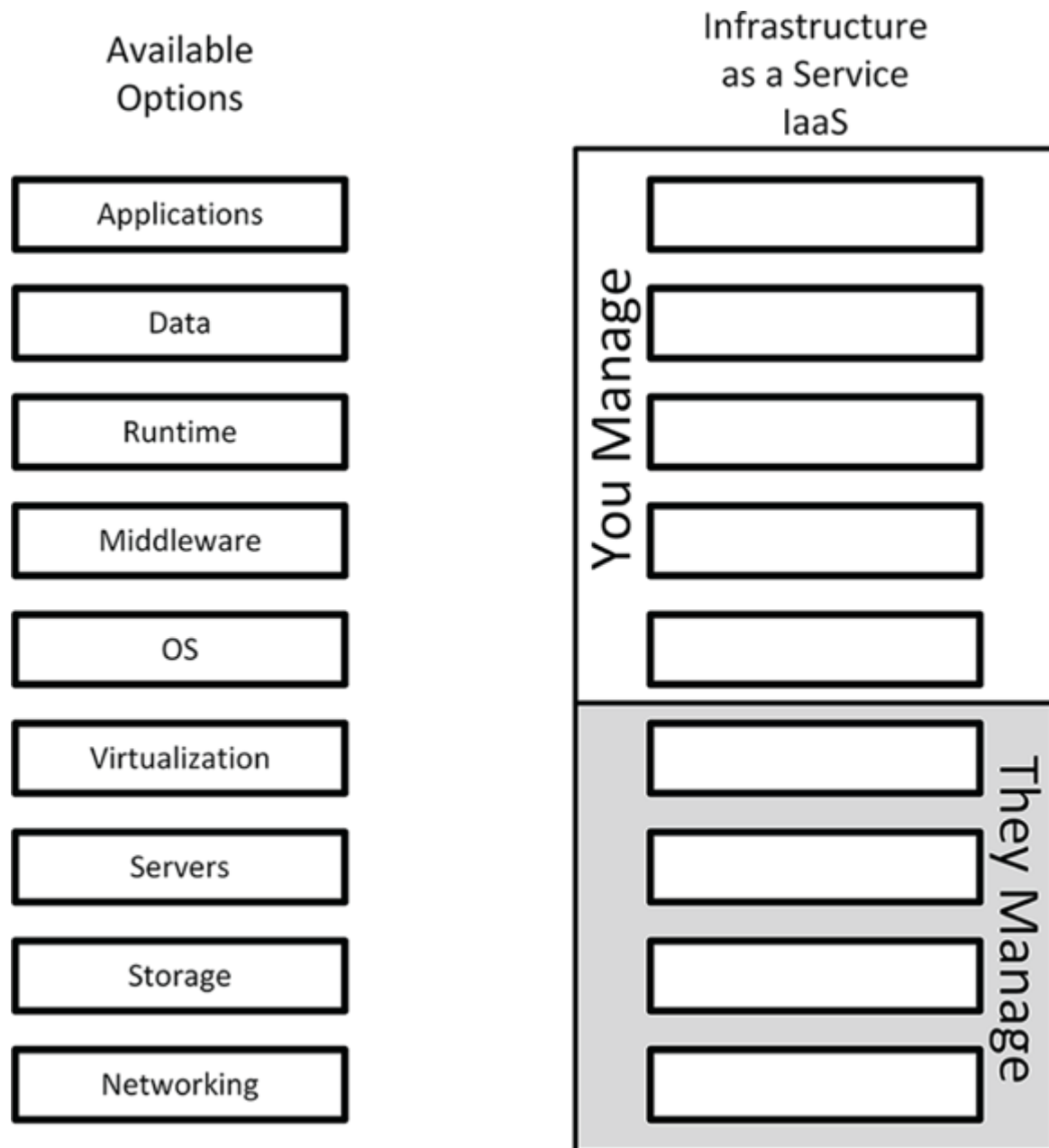
**5. Bill is setting up a computer that will be used to boot into several different operating systems. He would like to have one partition used for sharing or transferring data between the OSes. What file system should he use?**

- (A) FAT
- (B) FAT32
- (C) NTFS
- (D) Reiser FS

**6. What tool combines all Windows configuration and management tools into one place?**

- (A) Computer Management
- (B) Administrative Tools
- (C) Microsoft Management Console
- (D) Administrative Command Interface

- 7. What is the main protocol that is used by both Remote Desktop Connection and Remote Assistance?**
- (A) Dec/Net
  - (B) 802.11g
  - (C) SNMP
  - (D) RDP
- 8. You have been asked to evaluate virtualization solutions to be deployed in your corporate data center. Which one of the following is a solution you may consider?**
- (A) Citrix XenApp
  - (B) Microsoft Hyper-V
  - (C) VMWare Workstation
  - (D) Microsoft Remote Desktop Connection
- 9. The options on the left are the available components in an IaaS solution. Fill in the components in their correct location in the IaaS server model. Each choice will be used only once.**

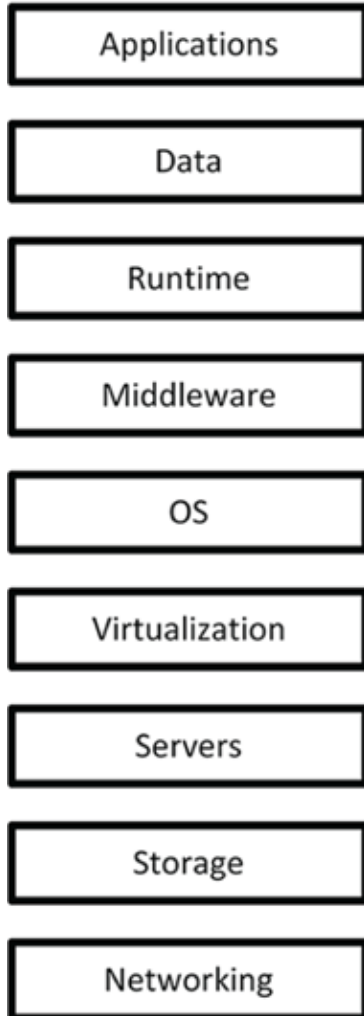


## Answers

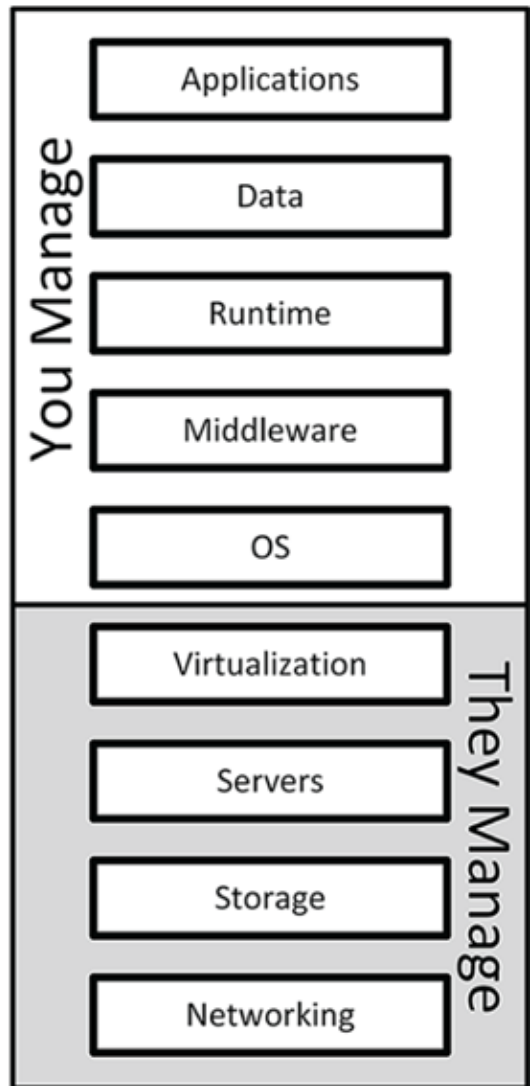
1. **B.** The Remote Assistance process starts with an invitation being generated by the person requesting help. This invitation is created using the Help and Support Center. See “[Remote Desktop Connection](#)” and “[Remote Assistance](#).”

2. **A, C.** Virtual memory is composed of both physical RAM and a swap or paging file on the hard drive. Review “[Paging your memory.](#)”
3. **B.** You can also launch the System Information tool by typing **msinfo32.exe** at the Run command. In addition to this, you can find the info on the System Properties, which can be opened by accessing the Properties of My Computer. Check out “[Checking the OS version.](#)”
4. **D.** Most blue-screen errors are the result of conflicts between processes running kernel mode, which would include device drivers. This is not to say that the multimedia application may not have made some unsupported calls to a sound or video card to cause the problem, but this would have been the second choice. Take a look at “[Getting into the architecture.](#)”
5. **A.** Although it has size limitations of 2 to 4GB depending on the OS used, the FAT system is the most compatible with different operating systems. Peek at “[Choosing your file systems.](#)”
6. **C.** Although Computer Management has a lot of management tools in it, it is itself a snap-in for the Microsoft Management Console (MMC). Administrative Tools are also a collection of preset MMC snap-ins. Look over “[Microsoft Management Console.](#)”
7. **D.** The Remote Desktop Protocol (RDP) is used by both of these tools. Study “[Remote Desktop Connection](#)” and “[Remote Assistance.](#)”
8. **B.** Microsoft Hyper-V is a server virtualization solution, while VMware Workstation is a desktop virtualization solution. Reread “*Virtualization Platforms.*”

### Available Options



### Infrastructure as a Service IaaS



9.



# Chapter 3

## Installing and Upgrading Windows

---

### IN THIS CHAPTER

- » Understanding boot methods
  - » Knowing the types of installation
  - » Partitioning and file systems
  - » Installing Windows
  - » Upgrading Windows
- 

Although installing an operating system (OS) has gotten easier over the last few years, it is still important to understand some of the issues surrounding installing and upgrading OSes.

This chapter gives you some background on the issues that surround the installation of Windows operating systems such as Windows 10. In this chapter, I walk you through these installations step by step and discuss the different phases of the installation process.

## *Understanding Installation Methods*

You can use a number of different techniques to install an operating system. But before I discuss the actual installation procedures, you should understand the overall approach you will take to install the operating system.

In the following sections, you find out about the different techniques that are used to invoke the installation of Windows operating systems. As an A+ Certified Professional, it is critical that you know a number of ways to invoke the installation so that you are well versed when the time comes.

## ***Bootable DVD***

With Windows OSes today, the DVD that you use to perform the installation is a bootable DVD, so you simply place the DVD in the system and power on the computer. When you power on the computer, the system will boot off the DVD and start the installation!

During the installation of modern Windows operating systems, you will have the opportunity to partition and format the drive from within the installation program itself. This is a huge benefit compared to older operating systems because those operating systems would make you partition the drive before you started the installation. Your goal now is simply to start the installation and take care of all partitioning and formatting tasks from within the installation.



TECHNICAL  
STUFF

Nowadays, with virtualization being such a popular option for systems administrators and even some end users, downloading Windows operating systems in the ISO disc image format presents a convenient way to replicate DVD boot functionality without having to mess with physical media.

To ensure that you do not install Windows over a perfectly functioning system, the folks at Microsoft built a feature into the installation DVDs for Windows so that if you boot from the DVD, you're asked to press a key (any key) before the installation process continues. This feature keeps you from unintentionally re-installing the OS if you accidentally leave the DVD in the drive.

## ***USB and PXE***

When planning to install the Windows operating system, you can invoke the installation by booting from media other than DVD. Today's systems can be installed by booting off a USB memory stick and invoking the installation. It will take time to prepare the USB stick so that it is bootable and contains the proper installation files.

Most systems today support the preboot execution environment (PXE), which is booting from a network card and then invoking the installation directly from the network without the use of a CD or DVD. To boot from the network, the system must have the following BIOS settings enabled:

- » **Boot from network:** Ensure that your system has the capability to boot off the network and make sure that network boot is enabled in the BIOS.
- » **Boot order:** Ensure that you modify the boot order and make the network your first boot device, then the CD/DVD, and finally the hard drive.

After this is set, you can then boot off the network by pressing F12 while the system is starting. The system obtains an IP address from the DHCP server on the network and then can connect to your installation media to perform the installation.

## *Network installation*

A number of network administrators install OSes and other applications to desktop systems via a network. When performing a network installation, you typically boot the system from bootable media (USB thumb drive, or perhaps a DVD) which then loads a network card driver and connects to a server on the network. More common in business environments, you can also connect to the network using PXE to perform the installation. Under the hood, modern Windows OSs store all the installation binary files in an archive format known as Windows Imaging (WIM). During an over-the-network installation, the WIM contents are streamed across the network to the target computer, where the actual installation takes place.

Network-based OS installation is performed every day by businesses not only on Windows PCs, but Mac and Linux systems as well. For example, NetBoot is an Apple macOS deployment technology that allows Mac computers to boot from their network interface card (NIC) firmware and download OS images from a central server. Windows PCs employ the Preboot Execution Environment (PXE) to do the same thing.

## *Drive imaging*

One of today's most popular techniques for installing an OS is to use imaging software, which creates a snapshot of a system and stores that snapshot in an image file. When you want to configure other systems with the same setup, you apply the image (snapshot) to the other systems. The contents of the image file overwrite the contents of the hard drive of the destination systems.

Here's an example of when drive imaging should be used: Your manager asks you to install Windows on 20 new computers. When you receive the systems, you sit down at one system and boot off your Windows DVD to perform a clean installation on that new computer (this computer is known as a *reference computer*). After the OS is installed, you install any additional drivers and applications that users will need. For example, most users need Microsoft Office, so you install Office on the computer as well.

After you have the system properly configured, you then create an image of that system by using imaging software, such as Acronis, Macrium, Symantec Ghost, or Microsoft's ImageX and DISM programs that come with the Microsoft Windows Assessment and Deployment Kit (Windows ADK). Typically, you would copy the image to an image server so that you can connect to the imaging server from across the network and apply the image to the other systems.

When it comes time to configure the other 19 systems, you boot off the network card or a bootable DVD or USB stick and connect to the imaging server and download the image to each of the 19 systems. This takes far less time than performing the installation of the OS, drivers, and applications on each system individually. Most companies today use imaging solutions.

## *Imaging with Windows 10*

Microsoft has a number of tools that can help you deploy Windows 10 on a number of computers, including its own imaging technology that you can use. To get a hold of the installation tools, you first must download the

Windows Assessment and Deployment Kit (ADK) from the Microsoft website.

Although CompTIA wants you to know about the ImageX command-line tool, you should know that Microsoft is gradually retiring ImageX in favor of its Deployment Image Servicing and Management (DISM) tool that does all the same things and more. Both tools are included in the Windows ADK.

### *Creating a bootable Windows PE disc*

The first step to working with Microsoft imaging tools such as ImageX to capture an image is to create a bootable CD known as a Windows Preinstallation Environment (PE) disc. A Windows PE disc is a bootable disc that runs a mini-version of Windows that is used to run programs like ImageX to image the system.

To create a Windows PE disc, follow these steps:

1. **Download and install the Windows ADK from the Microsoft website.**

Note that Microsoft publishes a separate version of the ADK for each OS. In other words, there are Windows 7, Windows 8.1, and Windows 10 versions available. Yes, this can get confusing!

2. **Choose Start ⇒ All Programs ⇒ Microsoft Windows ADK ⇒ Deployment Tools Command Prompt.**
3. **Type the following command to create a folder containing the 64-bit Windows PE boot files:**

```
copype.cmd amd64 c:\winpe_amd64
```

4. **Copy the base image to boot the CD/DVD from:**

```
copy c:\winpe_amd64\winpe.wim c:\winpe_amd64\iso\sources\boot.wim
```

5. **Copy ImageX to the ISO folder:**

```
copy c:\program files\Windows AIK\Tools\amd64\imagex.exe  
c:\winpe_amd64\iso
```

## 6. Create an ISO image from the ISO folder:

```
oscdimg.exe -n -bc:\winpe_amd\etfsboot.com c:\winpe_amd64\iso  
c:\winpe_amd64\winpe_amd64.iso
```

After the ISO file is created, you can then burn that to a CD or DVD and boot off it to create an image of a system with the ImageX program you placed on the CD.

### *Capturing an image with ImageX*

You can use Microsoft's `ImageX.exe` program to create images that come from the Windows ADK. After you have created your Windows PE boot disc, you can create an image of a system by following these steps:

1. **Install Windows on a system, and then install any drivers that are needed.**
2. **Install any applications that are needed, such as Microsoft Office.**
3. **Prepare the system by running `sysprep.exe`:**

```
c:\windows\system32\sysprep\sysprep.exe /generalize /oobe
```

This command is very important because it prepares the system for imaging by removing unique data from the system, such as the security ID and the computer name. The system is shut down and ready to image after the command completes.

4. **Boot off the Windows PE disc and connect an external drive to the system, which you will use to store the image on.**
5. **To create an image of a system, use the following command (in the code, the `Win7.wim` image is located in the path `E:\images`):**

```
imagex /capture c: e:\images\Win7.wim "Compaq Laptops - Windows 7"
```

This command creates an image of the C: drive and stores it in an `images` folder on the E: drive (the external USB drive).

## *Applying an image with ImageX*

After the image has been created, you can then apply the image to another system by following these steps:

1. **Boot off your Windows PE disc and create a primary partition on the target system with the following commands:**

```
Diskpart  
Create partition primary  
Format fs=NTFS label="Boot Drive" quick  
Assign letter=C
```

2. **Apply the image by using the following command:**

```
imagex /apply e:\images\Win7.wim 1 c:
```

In the preceding command, you are applying the first image that is inside the `Win7.wim` file to drive C: of the system.

3. **Make the drive bootable:**

```
Bcdboot c:\windows
```

Now that you understand a bit about imaging technology, I'll go back to performing a manual installation.

## *Preparing for Installation*

After talking to many people in the industry about installing different OSes or servers, I have come to realize that one thing that always requires more time is planning. Many people tell me that they can't do any actual work until their head office sends them the server. However, the best time to do your installation and disaster planning might be while the server is being shipped. Planning your installation or deployment of the OS to the desktops can save you time and money in the long run by helping you to anticipate any issues that might arise and to have the solutions ready when the time comes.

This section helps you identify some points you need to consider when installing a new Windows OS. Before jumping into the installation, be sure that you plan a number of installation decisions. Some things you will be asked about during the installation are

- » Hardware requirements
- » Computer name
- » Workgroup/domain
- » Partitions
- » File systems
- » Application support

### *Hardware requirements*

You first prepare to install an OS by finding the OS's hardware requirements and making sure that the computer fits the bill. [Table 3-1](#) shows the minimum hardware requirements for Windows 10.

**TABLE 3-1 Windows 10 Hardware Requirements**

<i>Hardware Component</i>	<i>Windows 10</i>
Processor	1-GHz processor (32- or 64-bit)
Minimum memory	1GB (32-bit); 2GB (64-bit)
Hard drive space	16GB (32-bit); 32GB (64-bit)

Not only should you verify that the computer meets the minimum hardware requirements before installing an OS, but you should also make sure that the hardware components you are using will work with the OS. For example, make sure that the make and the model number of your network card are compatible with the OS you want to install. For years, Microsoft published a list of hardware components that had been tested with each version of its operating systems. You can find the HCL for a given OS on the Windows installation CD in the `hcl.txt` file, or you can find the listing online at the Microsoft website.



Nowadays Microsoft calls the HCL the Windows Certified Products List (CPL), and it is (wisely) completely web-based. The CPL is not a list of the only devices that will work with Windows; it is a list of devices that have been tested. If you have a network card that is not on the CPL list, it might still work with the OS, but it hasn't been tested. There is only one way to find out whether it works — install it! Just make sure you are installing it on a test system and not a production system, just in case it causes the system to crash.

## *Computer name*

When you install Windows, you must specify a computer name for the machine you are installing. This computer name is a unique name assigned to the system and will be used to identify the system on the network. You want to plan the computer names because you are not allowed to have two Windows systems on the network with the same name. The computer names can be up to 15 characters, and they are not allowed to include spaces. For more information on computer names, check out Book 8, [Chapter 3](#).

## *Workgroup/domain*

When installing Windows on a system, you need to specify the workgroup or domain that you want the system to be a part of. A *workgroup* is a logical grouping of computers. For example, you could logically organize all the accounting systems into an accounting workgroup — the benefit being that when users browse the network for resources, they can double-click the accounting workgroup to access all computers in the accounting workgroup.

If you are installing Windows into a Windows domain, you need to specify the domain name instead of the workgroup name during the installation. A *domain* is the term that Microsoft uses for its networking environments. A domain has a central server that stores all the user accounts so that users have to log on to the domain only once to access resources across a network.

If you are not sure whether you are installing your Windows system into a workgroup or a domain, choose a workgroup. You can always join the

domain later by going to the properties of My Computer. For more information on changing a computer name, check out Book 8, [Chapter 3](#).

## *Partitions*

When you install Windows, you need to partition the hard drive or select which partition you want to install Windows to. Plan this ahead of time! *Partitions* are logical divisions of the hard drive that you can use to help separate the different types of information stored on the system.

The following is a review of partition types you can read about in Book 2, [Chapter 5](#):

- » **Primary partition:** A partition that you can boot from.
- » **Extended partition:** A method to extend beyond the four partition limitation. You can create an extended partition to hold a large number of logical drives.
- » **Logical drives:** An area of space in the extended partition that is formatted and assigned a drive letter.

For more information on partitioning a hard drive, check out Book 2, [Chapter 5](#).

The default disk type when installing Windows is a *basic disk*, which supports up to four partitions per disk. You can convert the drive to a *dynamic disk* after installation and then create a number of volumes on the drive.

When installing Windows, you can manage the partitions from within the Windows setup program instead of having to boot from a startup disk first and then create the partitions before installing the operating system, like you had to do in the old Windows 9x days. You can build all your partitions from within the setup program.

Within the Windows setup program, you can build the partitions by choosing an area of free space and then pressing C (for create). The setup program then asks you the size of the new partition. You want to be sure that you create a partition that is large enough to hold the operating system and any future patches or updates to that operating system. For example,

the laptop I am using to write this book has a 500GB hard drive. I have created a partition to hold the operating system, which is 120GB in size. By the time I have installed the operating system, patched it, and installed my applications, I only have 50 percent of that space available for future updates. Windows 10 allows you to create partitions using a graphical screen within the setup program.

The Windows setup program also offers a Delete command, which lets you delete any existing partitions. After creating the partitions and choosing a partition in which to install the Windows OS, you are asked what file system you want to use.



TECHNICAL  
STUFF

When you install Windows, you don't have any control over the types of partitions that are created during the setup. For this reason, it is best to only create one partition (to install the OS on) during the installation. Then, after the OS has been installed, use Disk Management to create the remaining partitions. You will get more options and flexibility from the Disk Management console than from the Windows installation program.

## *File systems*

Windows supports four file systems: exFAT, FAT, FAT32, and NTFS. The primary advantage of using the FAT file system is that it is common to all Windows OSes. The FAT file system has its limitations, however, in that it can handle only up to 2GB partitions. The FAT32 file system, however, supports up to 2000GB partitions (although the Windows setup program cannot create a partition larger than 32GB with FAT32).

exFAT is a Microsoft-proprietary file system that's optimized for use with a flash drive. exFAT is a great fit for smaller drives that aren't a good fit for NTFS.



**WARNING** Neither version of FAT supports security features, so beware of these file systems!

NTFS (New Technology File System) is a file system supported by Windows that offers a richer set of features than FAT or FAT32. For example, NTFS supports setting permissions on folders and files so that you can control who can access what files. NTFS also supports auditing, compression, encryption, and quotas — a feature that allows you to limit how much hard drive space a single user can use. None of these features are available with FAT or FAT32. If you need any of the features provided by NTFS, you need to use an NTFS file system on each partition.



**FOR THE  
EXAM**

For the A+ exams, be sure to be familiar with the different file systems that Windows supports. Also note that NTFS is the only file system that gives you features such as permissions, auditing, and quotas.

Another file system that you should be familiar with for the A+ certification exams is the Compact Disc File System (CDFS). This file system allows the operating system to access the data on optical drives, such as CD-ROMs or DVDs.

## **FULL FORMAT VERSUS QUICK FORMAT**

When you perform a clean Windows installation, you're given the choice to format the hard drive before laying down the operating system. A quick format simply erases the disk but does not perform any error-checking.

By contrast, a full format not only erases the partition content, but also takes additional time to ensure that every cluster, or allocation unit, can reliably hold data. What I suggest to customers is that they choose the quick format option unless they have reason to believe the disk may be unreliable, in which case I recommend performing a full format.

## *Non-Windows file systems*

For completeness, you should be aware of some of the other major file systems in use:

- » **HFS:** Hierarchical File System, developed by Apple for use with macOS and Apple's desktop and laptop computers. The current version of this file system, HFS Plus, is called Mac OS Extended from within the operating system.
- » **ext3, ext4:** File systems native to the Linux operating system. Traditionally Linux creates a separate ext3 or ext4 partition for use as a virtual memory paging file; this file and partition are known as a swapfile or swap partition.

You need to install a special driver in Windows in order to read HFS+ and/or ext file systems. This can be useful, for instance, when you're tasked with recovering files from a hard drive formatted with a non-Windows file system.

## *Other preparation steps*

Before you install Windows to your production systems, you also want to make sure that you prepare for the installation by checking that the applications that are going to run on the systems work and that your UEFI/BIOS is prepared to boot from DVD. This section outlines these two additional preparation steps.

## *Application support*

Make sure that you test each application that will be running on the OS completely to verify that it functions correctly. Today, you may have a mix of some 32-bit applications and some 64-bit applications. Windows stores 32-bit programs in the path `C:\Program Files(x86)` by default, and it stores 64-bit programs in the path `C:\Program Files`.

Be sure to test each application with the new operating system you are installing. For more information on application support in Windows, check out Book 6, [Chapter 2](#).

## *BIOS/UEFI*

When you install the Windows OS, you will boot from the Windows DVD, and the setup program will start. Because you are booting from a DVD, you need to prepare for the installation by verifying in the BIOS/UEFI settings that the DVD device is the first device in the startup order. This ensures that you can boot off the Windows setup media. For more information on configuring BIOS/UEFI, check out Book 2, [Chapter 4](#).

### *Other considerations*

You want to consider a number of things when planning your installation of the Windows operating system. The following items should be planned carefully:

- » **Repair installation:** The great thing about the Windows installation DVD is that it is also used to repair a corrupt installation of Windows, so keep that installation DVD handy!
- » **Multiboot:** If you need to support older applications that will not run on the new version of Windows you are installing, you may need to install Windows in a dual-boot configuration. If installing Windows 7 in a dual-boot configuration, be sure to install it on its own partition.
- » **Remote network installation:** As mentioned earlier, you can install Windows across the network. If you are planning to install from across the network, be sure that the system has been prepared to boot off the network card on the system.
- » **Image deployment:** The best way to install an operating system is to prepare an image to be installed. Spend some time preparing images of your systems to simplify the installation at a later time.
- » **Third-party drivers:** Your new Windows installation may not have drivers for the hardware in your computer, so be sure to spend some time downloading new drivers from the vendor's website.
- » **Time/date/regional settings:** Ensure that you set the date and time settings on the system during installation.
- » **Factory recovery partition:** When partitioning the system, do not overwrite any of the default partitions, created by the manufacturer of

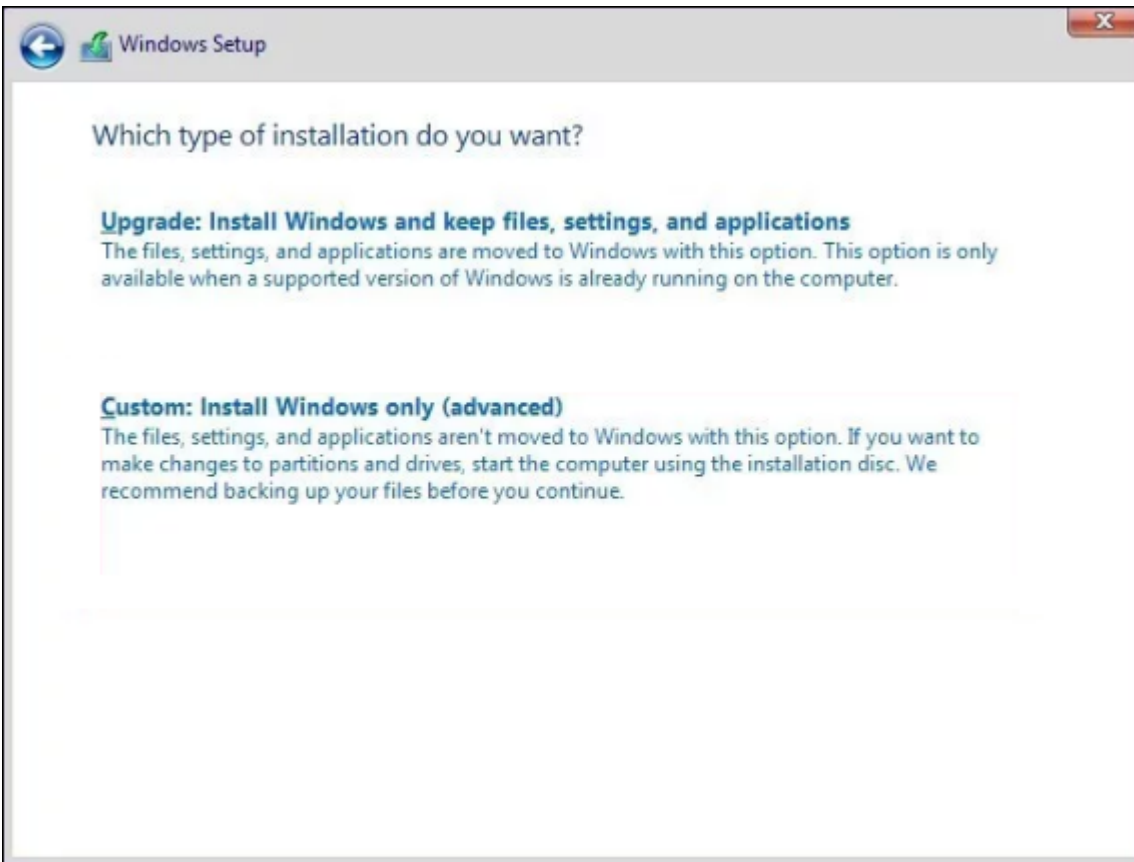
the system, that have the recovery tools; these partitions are needed if you intend to recover the system to its original state.

- » **Automatic Updates:** Ensure that you enable automatic updates so that your system is updated on a regular basis. This will help improve the security of the system.

## *Performing Attended Installations of Windows*

An attended installation of the OS is an installation that you attend, or sit through, and answer all the questions that the setup program asks. For Windows 10, Microsoft followed the same installation paradigm as with Windows 7 and even Windows 8.1, but streamlined the process even more. In a nutshell, here is the information you're required to specify when you perform a manual installation of Windows 10:

1. **Accept the license agreement.**
2. **Choose an upgrade or clean installation.**  
[Figure 3-1](#) shows this window.
3. **Select the installation partition and optionally format it first.**
4. **Name the computer.**
5. **Choose Windows Update and Internet Explorer configuration options.**
6. **Create a Microsoft account or a local administrator account.**



**FIGURE 3-1:** Installing Windows 10 has never been easier to do.

Thanks to Windows PE, you have access to the Internet and local network as soon as Windows loads a network interface card (NIC) driver. This means you can patch your Windows 8.1 installation immediately.

I remember the days when I'd install Windows XP completely offline because if I had an open Internet connection on the box before updating it, the machine would attract malware almost automatically. Those were the bad old days.

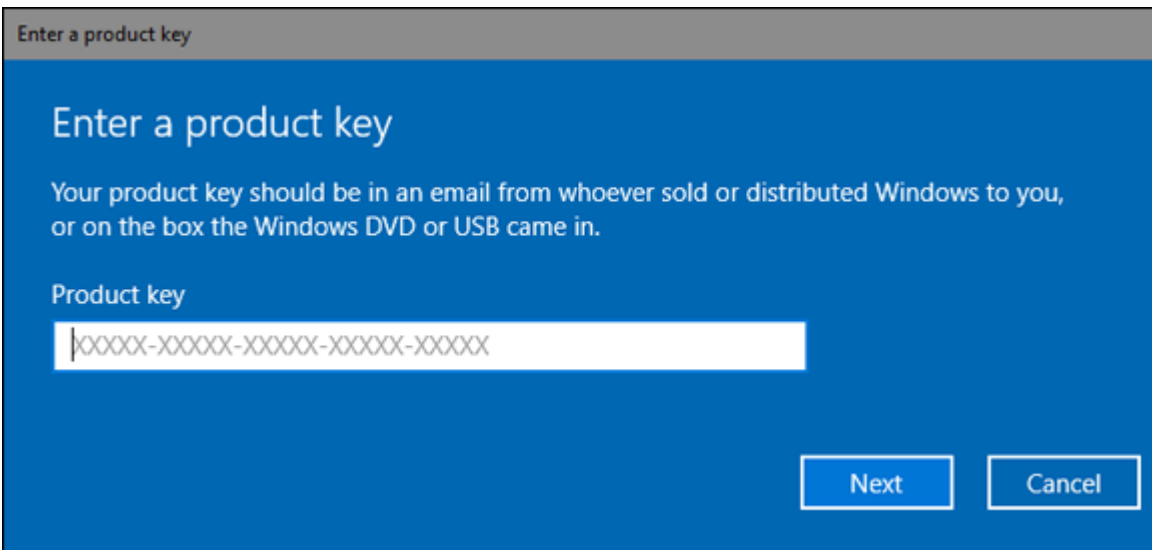


**WARNING** Be careful when you choose to format a volume during Windows setup — any data previously on that volume will be irretrievably erased.

After you finish installation, two common post-setup actions are setting the time zone and activating the software with Microsoft. You can perform



both tasks by opening Start and clicking the gear icon to open the Settings panel. I show you where to enter a product key in [Figure 3-2](#).



**FIGURE 3-2:** Activating Windows 10 in the Settings panel.

## *Performing Unattended Installations of Windows*

An unattended installation (compared with an attended installation) frees you from having to be present when the installation is run. Before installation, you place all the answers to the installation questions in a text file, and the setup program reads the text file.

To automate installing Windows 10, you use different tools than with the previous OSes mentioned. The concept is pretty much this: You still need to build an answer file, but the tools you use are a little different.

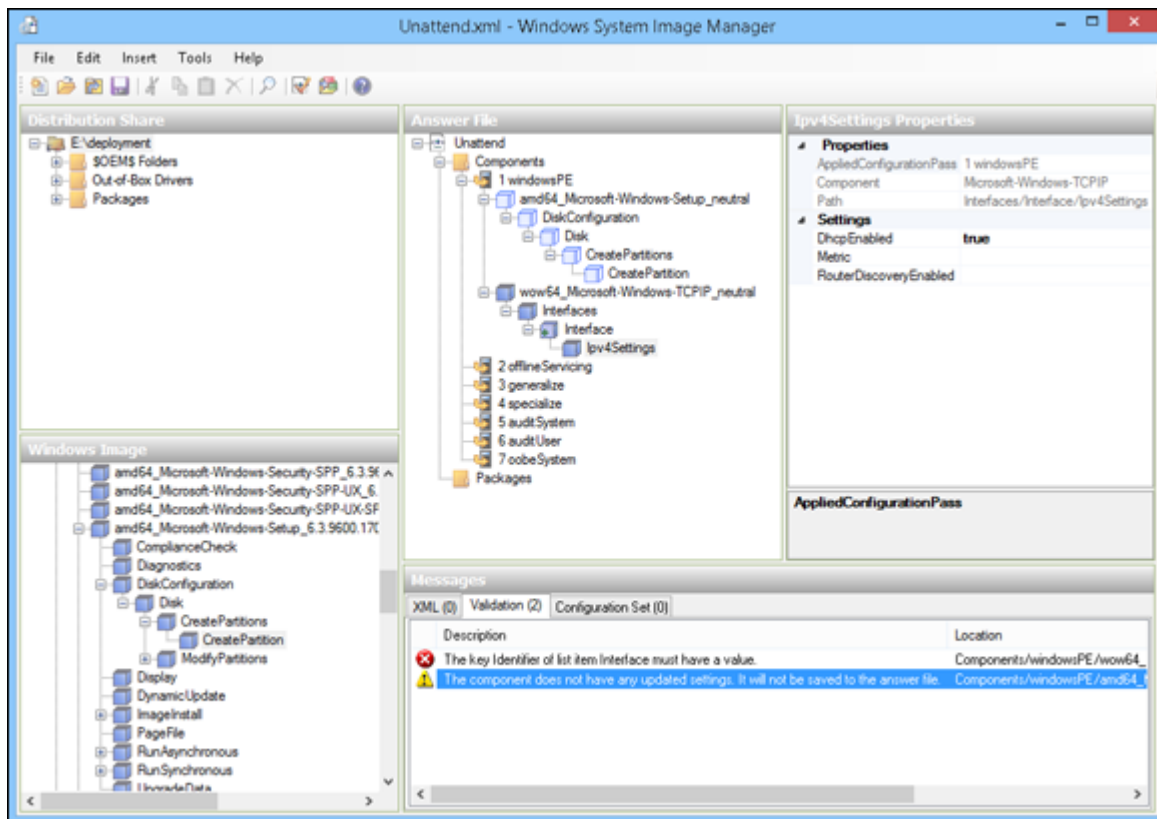
The first change that Microsoft made with automating Windows Vista setup (all those many years ago!) is that the answer file is no longer a TXT file. It is now an Extensible Markup Language (XML) file! (An XML file is a plain text file supported by a number of different products.)

To create an answer file for Windows 10 installations, download the Windows ADK from the Microsoft website. In the Windows ADK is the

Windows System Image Manager (SIM) tool, which you use to create an answer file to automate Vista installations.



**WARNING** Learning the Windows SIM, shown in [Figure 3-3](#), takes some patience; the interface is something that only a true software developer could love.



**FIGURE 3-3:** Use Windows System Image Manager (SIM) to create an unattended answer file for Windows 7 or Windows 8.1 automated installations.

Once you create your unattend.xml file, you can copy the file to a USB thumb drive and boot the target computer from the Windows DVD. As long as (a) you have the answer file in the root directory of the USB stick and (b) the USB stick is plugged in and recognized by your computer, Windows setup will “automatically” reference the answer file when it requires input.

# *Verifying and Troubleshooting the Installation*

In the previous two sections, I show you how to perform attended and unattended installations of Windows. In this section, you look at some tips for verifying and troubleshooting a Windows installation.

First things first. After Windows is installed, ensure that all device drivers have been installed. Open Device Manager and verify that all drivers are present. If you are missing drivers for some devices, Device Manager will have a category called Unknown Devices, which are indicated by a yellow question mark.



**TIP**

Check out Book 6, [Chapter 1](#) to find out more about updating drivers.



**REMEMBER**

Windows creates a number of log files during installation. If installation does not go as you planned, peruse these logs for more information about an error. These log files report information only for events that happen during the installation, so if you're troubleshooting something like booting Windows or networking, these files won't help.

The log files created during installation are

- » `Setupact.log` records information about the files that are copied during installation.
- » `Setuperr.log` records information about errors that happen during installation.
- » `Setupapi.log` records information about device driver files that are copied during installation.

- » `Setuplog.txt` records additional information about the device drivers.
- » `Sessions.xml` records all servicing activity.
- » `CBS.log` records more details about offline servicing failures.



FOR THE  
EXAM

Be sure to remember the log files that are created when you install Windows. These files can be used to help troubleshoot problems with the installation of Windows.

A number of problems may arise during Windows installation. The following list outlines a few common ones:

- » **Bad DVD or DVD device:** If you experience failure to copy files during the setup process, you might have a bad DVD device, or maybe the DVD itself is bad. Try booting from another Windows DVD to find out whether the problem is with the media or the DVD device.
- » **Can't boot after install:** If you have trouble rebooting after you complete an installation, be sure that you did not leave a floppy disk in the floppy drive. Also check BIOS/UEFI setup to ensure that the hard drive appears as a boot device. (See Book 2, [Chapter 4](#) to find out how to tweak BIOS/UEFI settings.)
- » **Can't start Windows install:** If you can't start the Windows setup by booting off the installation media, make sure that the DVD device is listed as a startup device in BIOS/UEFI. Also, ensure that the DVD is listed before the hard disk in the system boot order.
- » **RAID not detected during installation:** When installing Windows, if you have a hard drive controller or a RAID controller in the system that is not detected during installation, press F6 during installation to supply third-party drivers.
- » **Not enough disk space:** The Windows setup program checks available hard disk space. If your computer doesn't have enough

space, Windows indicates this with an error, and the Windows installation stops. You will need to restart the installation again after cleaning up disk space.

Overall, Windows installations have become more reliable with each successive version, so you are less likely to have installation problems with the current version than you would have back in the Windows XP/7 days.

## *Upgrading Windows*

You will be responsible for understanding how to upgrade from previous versions of Windows to Windows 10. The following sections introduce you to the theory of upgrading an OS.

### *Preparing to upgrade*

Many businesses run Windows, so understanding how to upgrade is important. Whether installing the OS from scratch or performing an upgrade, the process is pretty much the same. **Note:** With an upgrade, though, you will find many installation decisions already made for you during the installation of the previous OS. For example, when you upgrade an older version of Windows, you will not be asked the computer name of the system as this information is inherited from the previous operating system installation that you are upgrading.



**WARNING** Before you upgrade any OS, backup *the system and any important data*. You never know when an upgrade is going to go bad, so make sure you can at least put the system back to its previous state.

### *Upgrading to Windows 10*

According to Microsoft, you can perform a direct upgrade to Windows 10 from Windows 8.1. You can perform an in-place upgrade to Windows 10 from Windows 7 or Windows 8.1.

Remember that an upgrade installation of Windows intends to preserve all user settings and document data. That's the benefit. That said, please don't fall victim to the mistaken idea that upgrading Windows to a new version will fix the so-called "ghosts in the machine" that plagued the initial Windows version.

In this case, I suggest you back up all user data and preferences and perform a clean installation of the newer Windows version.

## *Installing or Removing Additional Windows Components in Windows 10*

After installing Windows, you can add or remove components (or portions of the Windows OS) by going through the Programs and Features control panel. For example, if you would like to create a website, you will most likely want a web server installed on your system. Windows does not come with web server software installed by default, so you would need to add one after you install the OS.

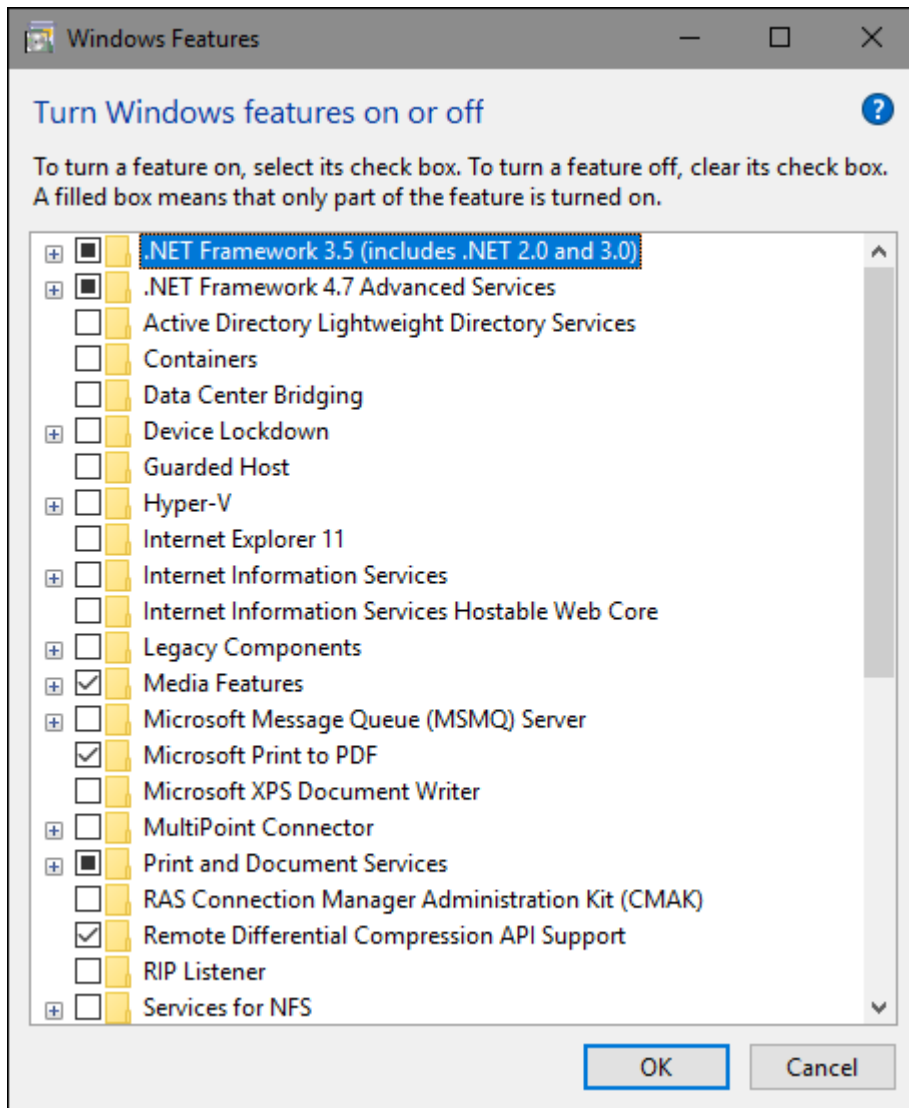
To install additional Windows components after the installation of the operating system, follow these steps:

- 1. Open the Program and Features control panel by navigating to the Start Screen, typing program and features, and pressing Enter.**
- 2. In the Programs and Features dialog box, click Turn Windows Features On and Off.**

The Windows Features dialog box appears, as shown in [Figure 3-4](#).

- 3. Select each component to install or uninstall and then click Next.**  
Windows 10 stores installation files in the local file system, so you shouldn't be prompted to mount the installation media.
- 4. After the files are copied, click Finish.**

5. Close the Programs and Features dialog box and restart the computer if necessary.



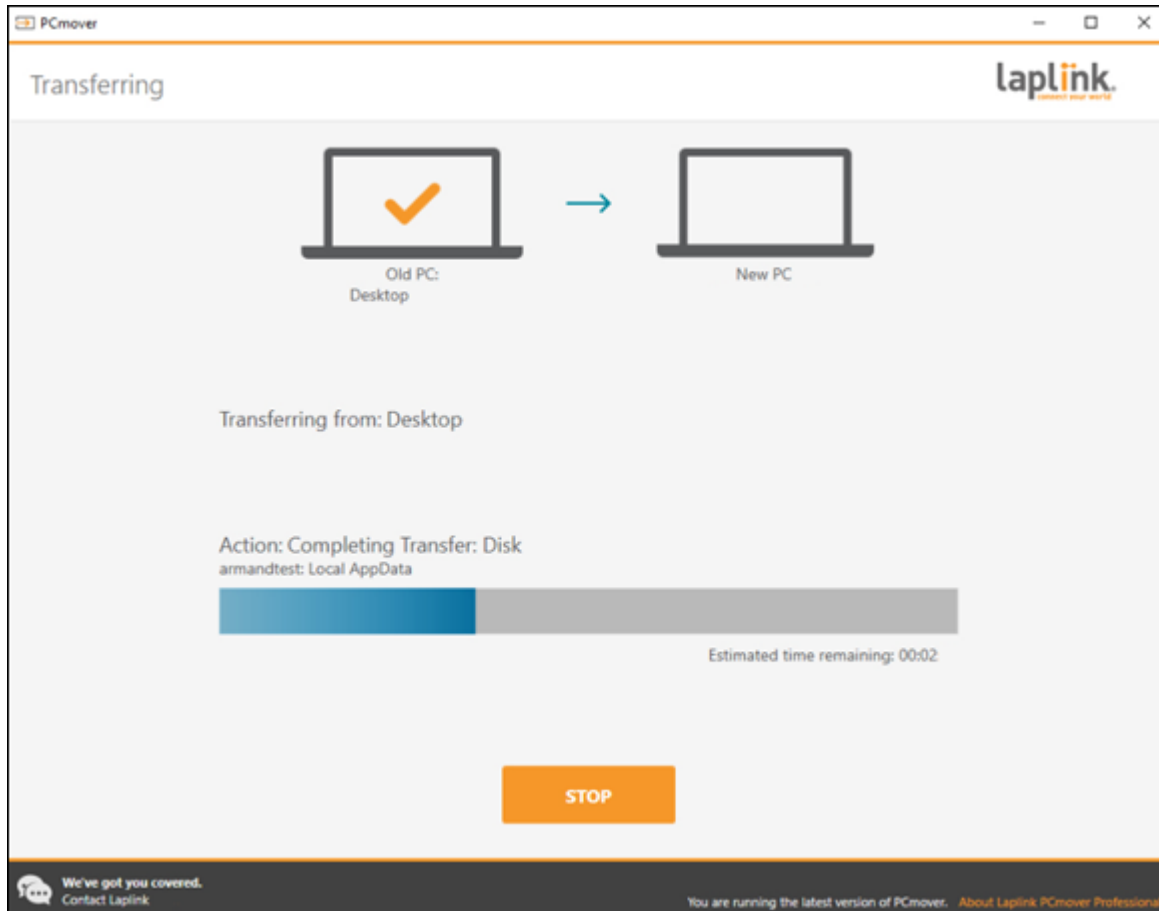
**FIGURE 3-4:** Installing additional Windows components in Windows 10.

## *Restoring User Data Files*

Microsoft once had a built-in program called the Easy Transfer Wizard to make it easier to move your files and preferences between two computers.

In Windows 10, however, we must purchase a license for an external product to do that.

The software is called Laplink PCmover Express. The software includes a double-headed USB cable that you use to connect your two computers (assuming you are migrating your data files to another system instead of restoring backed-up files to the same system). I show you the interface in [Figure 3-5](#).



**FIGURE 3-5:** Installing additional Windows components in Windows 10.

## *Getting an A+*

This chapter introduces you to some of the guidelines for installing the different Windows OSes. Some key points to remember are

- » When planning your installation, be sure to plan the partition size, file system, and the computer name that you will use when installing Windows.



- » You can boot off the Windows DVD or ISO virtual disc to invoke an installation.
- » Modern Windows OS versions rely upon the Windows PE environment to streamline the installation and initial configuration processes.
- » To dual-boot multiple operating systems, make sure that you are using a file system common to each OS, and then install each OS to a different partition.
- » The user state migration tools are used to copy a user's settings and files from one computer to another. A great feature to make your life easier if you need to do this someday!

## *Prep Test*

**1. You want to create an image of a Windows 10 installation. What program would you use?**

- (A) `scanstate.exe`
- (B) `dism.exe`
- (C) `oscdimg.exe`
- (D) `copyype.cmd`

**2. What format does Windows use for unattended answer files?**

- (A) XML
- (B) HTML
- (C) EXE
- (D) CMD

**3. What is the command used to remove unique data from a system before it is imaged?**

- (A) `dism.exe`
- (B) `imagex.exe`
- (C) `oscdimg.exe`

(D) `sysprep.exe`

**4. Where would you go in Windows 10 to install additional operating system components after the installation is complete?**

(A) Add/Remove Programs

(B) System icon

(C) Programs and Features

(D) You can't install additional operating system components after the OS is installed.

**5. What is the minimum RAM requirement for 64-bit Windows 10?**

(A) 768MB

(B) 1GB

(C) 2GB

(D) 4GB

## *Answers*

1. **B.** You can create an image of a Windows 10 machine with `dism.exe`, which comes with the Windows ADK. Review “[Applying an image with ImageX](#).”
2. **A.** The Windows System Image Manager (SIM) tool, which is a component in the Windows ADK, uses the Extensible Markup Language (XML) as its file format for unattended answer files. Peruse “[Performing Unattended Installations of Windows](#).”
3. **D.** `Sysprep.exe` is used to prepare a system for imaging by removing unique data from a system. Take a look at “[Capturing an image with ImageX](#).”
4. **C.** To install additional Windows components in Windows 10, go to Programs and Features in the Control Panel. Peek at “[Installing or Removing Additional Windows Components in Windows 10](#).”

5. **D.** Although you can install Windows 10 on a 32-bit CPU-equipped computer with only 1GB of RAM, you need at least 2GB RAM for a 64-bit system (which the vast majority of computers today are). *Look over “[Hardware requirements](#).”*

# Chapter 4

## Managing Files and Directories

---

### IN THIS CHAPTER

- » Working with files and directory structures
  - » Working with Folder Options
  - » Understanding file-naming conventions
  - » Comprehending file attributes
- 

Most people agree that money management is important: When you put your money somewhere, it's good to have an organized system so you can remember where the money is and retrieve it as needed. Similarly, file management is an important part of any operating system. You need a way to organize the data on your drive so that it is easily retrievable, as well as a way to identify files that are used for certain purposes.

With the changes that the Microsoft-supported file systems have undergone over the years, an A+ Certified Professional needs an understanding of all the file systems because it is highly likely that the computers a professional is called to work on will not all be running the most current OS. In many cases, the computers that require recovery will be running the oldest OS or will have users on the bleeding edge, trying to make use of the newest features of the latest version of Windows.

In this chapter, you get a brief history of file-naming conventions and how they have changed (and, in some cases, stayed the same) over the years. I also tell you what you need to know about file identification and file management and give you an overview of the file attributes associated with the various Microsoft file systems that have come and gone since the days of MS-DOS 1.0.

# Identifying File-Naming Conventions

File-naming conventions have undergone several changes over the years. In this section, you get a look at where they have been and where they are now. You also take a look at the differences between filenames and directory entries.

When MS-DOS was the premier OS on the market, it set the standard of the eight-dot-three (8.3)–character filename. This file system was created by using 32 character fields (bytes) for the filenames. If you work out the math, you’re probably wondering where the extra characters are. Well, 8 plus 3 is 11, and that leaves 21 outstanding characters (bytes). [Table 4-1](#) summarizes how each byte is used.

**TABLE 4-1 Directory Entry Format**

<i>Use</i>	<i>Size</i>
Filename	8 bytes
Extension	3 bytes
Attribute	1 byte
Reserved	10 bytes FAT 32 uses two of these bytes.
Time	2 bytes
Date	2 bytes
First cluster	2 bytes
Size	4 bytes



FOR THE  
EXAM

The File Allocation Table (FAT) is an index on your file system that holds a pointer to where each file is stored on your hard drive. On an NTFS (NT file system), this index is called the Master File Table (MFT). To move a file on a file system, you only need to change its reference in the table, and not its location on your drive. This is why moving files between folders is so fast, while copying them is very slow.



TIP

With every system or component used in a computer, there is a limit; sometimes it is a very large limit, but a limit, nonetheless. That limit is always based on a binary number. Computer systems have RAM limits of 2, 4, 8, or 16GB — never 7.5GB because that is not a binary number. The binary number system is also referred to as Base 2, as compared with our traditional number system, which is Base 10.

Common Base 2 numbers are determined by their digits. For instance, a four-digit Base 2 number has a maximum value of 1111. The following equations figure the value of each digit, from left to right:

$$1 \times 2^3 = 1 \times 8 = 8$$

$$1 \times 2^2 = 1 \times 4 = 4$$

$$1 \times 2^1 = 1 \times 2 = 2$$

$$1 \times 2^0 = 1 \times 1 = 1$$

Then, when you sum the value of each digit ( $8 + 4 + 2 + 1$ ), you get 15. Considering that you could have 0000 as a possible value, there are 16 possible values: 0 through 15. When you count the number of possible values for 1-digit to 12-digit Base 2 numbers, the value limits you end up with are 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, 2048, and 4096.

In cases where the limit is not based on a binary number, some overhead is usually involved. NetBIOS (Network Basic Input/Output System) computer names are 15 characters long, but they fit into the binary system because there is a 16th character used to identify the type of name, and 16 is a common binary limit. As I mention earlier, filenames are 8 plus 3 characters long, which is only 11 characters or bytes in length. However, the name is only part of a directory entry, and the entire entry is 32 bytes long, and 32 is a round binary number.

When dealing with file attributes, one byte (8 bits) stores all attribute settings. (For more information on file attributes, see the section “[Understanding File Attributes](#),” later in this chapter.) There are not, however, eight attributes.

The 8.3-character naming convention quickly proved to be very limiting. Extensions were often used to allow for longer names and were not directly associated with individual applications. When Windows came onto the market, people began using file extensions properly. Within Windows, the extension was used to identify the application that created a particular document.

Other OSes placed different limits on the length of filenames. For example, Mac (before OS X) limited the length of filenames to 31 characters, and OS X limited them to 255 characters. Although 8.3 was very limiting, 255 characters seems excessive, but you likely won’t be limited in your choice of filenames.

## ***Long and short filenames***

Windows-based OSes both allow for long filenames on a FAT16 partition. These filenames are limited to 255 characters, but some applications (such as different versions of Windows Explorer) may not be able to display the entire filename. Some older versions of Explorer were only able to display 220 characters, including the period separator for the file extension. However, with Windows 7 Explorer and newer OSes, the full 255 characters of the filename can be displayed. With older OSes, if you want to use names longer than Windows Explorer can display, you have to use a different application.

On a FAT16 or FAT32 partition, you are still limited to the 8.3 naming convention. Windows OSes get around this problem by cheating the file system. When you save a file, it is saved by using one directory entry and a short 8.3-character filename. The short filename is created by using the first six characters of the filename followed by a tilde (~) and an incremental number. After creating four files with the same six starting characters, the formula for creating short names is changed. The first two characters are used, which are then followed by either a randomly or sequentially generated four-digit hexadecimal number (depending on your OS), followed by a tilde (~) and the number 1.

[Table 4-2](#) lists the names of six files and their short filenames that were created in the same directory on a Windows 7 system. To get a listing of the short filenames, you can use `dir /x`.

**TABLE 4-2 Short Filenames in Windows 7**

<i>Long Filename Entry</i>	<i>Short Filename Entry</i>
ShortFileTest1.txt	SHORTF~1.TXT
ShortFileTest2.txt	SHORTF~2.TXT
ShortFileTest3.txt	SHORTF~3.TXT
ShortFileTest4.txt	SHORTF~4.TXT
ShortFileTest5.txt	SHEB78~1.TXT
ShortFileTest6.txt	SH07E0~1.TXT

You have now seen how short filenames are generated, but the question about where the long filenames are stored on FAT16 and FAT32 partitions still exists. The long filenames are stored in additional empty directory entries. The characters for the long filename are stored using 11 characters per additional directory entry. So, a file with a name of

```
My financial report for 2000.txt
```

takes one directory entry of the short filename (possibly `myfina~1.txt`) and one additional entry for each of the 11 characters in the filename, or an additional three entries. That means that this one file would actually

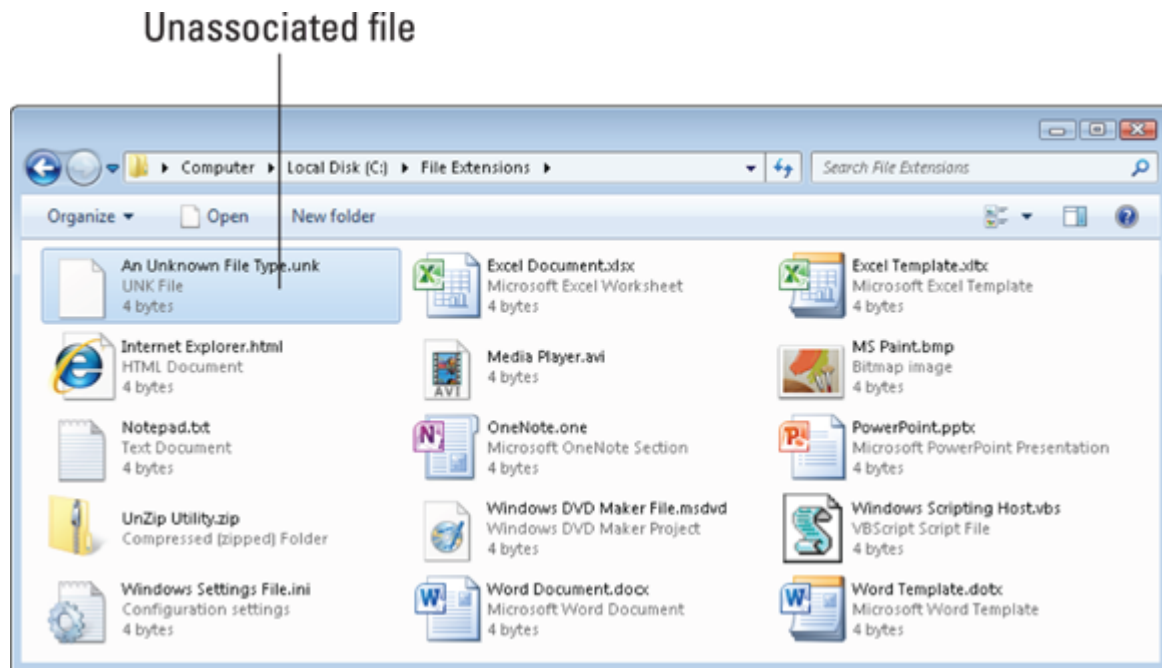


occupy four directory entries on your drive. These long filename directory entries have a nonstandard attribute combination of Read-only, Hidden, System, and Volume Label. Although many files on your disk might have a combination of Read-only, Hidden, and System, Volume Label is usually used alone and only on one directory entry that stores the Volume Label for the disk. By using all four attributes, they are a nonstandard combination — and if non-Windows systems see these entries, they ignore them rather than generating an error.

One of the problems with long filenames occurs when the long filename entries disappear. This can happen if you use older disk utilities on your disk. Some of these utilities will tell you that you have a problem with your directory entries and offer to fix them. “Fixing,” unfortunately, means deleting all the “invalid” entries, which means you lose all your long filenames. This is not a good thing.

## *Creating file associations*

Generally speaking, an *association* is a link between two separate things. *File associations* link the file extensions of filenames to the programs that can be used to open the files. When dealing with Windows, file associations let the OS know what program should be used to open a specific type of file. This information is stored in the Registry but can be accessed from a number of locations. The *Registry* is a central location that stores configuration and settings for Windows. Any files not associated with an application will have a generic Windows icon (see [Figure 4-1](#)).



**FIGURE 4-1:** Each file has an icon that represents its file association.



**TIP**

Before macOS, Mac systems did not use file extensions for associations. Instead, each file was saved with both a data and a resource portion. The resource portion contained the file type and associated application information. Windows-based files are saved only with a data portion. In macOS, files no longer contain a resource portion, and use file extensions to define types of files.

There are a number of different ways in Windows to associate file types with applications:

- » **Double-click unassociated files and assign an application in the dialog boxes that follow.**
- » **Press Shift while right-clicking associated files and choosing an Open With option.**
- » **Use the Folder Options dialog box.**
- » **Edit the Registry.**



**TIP**

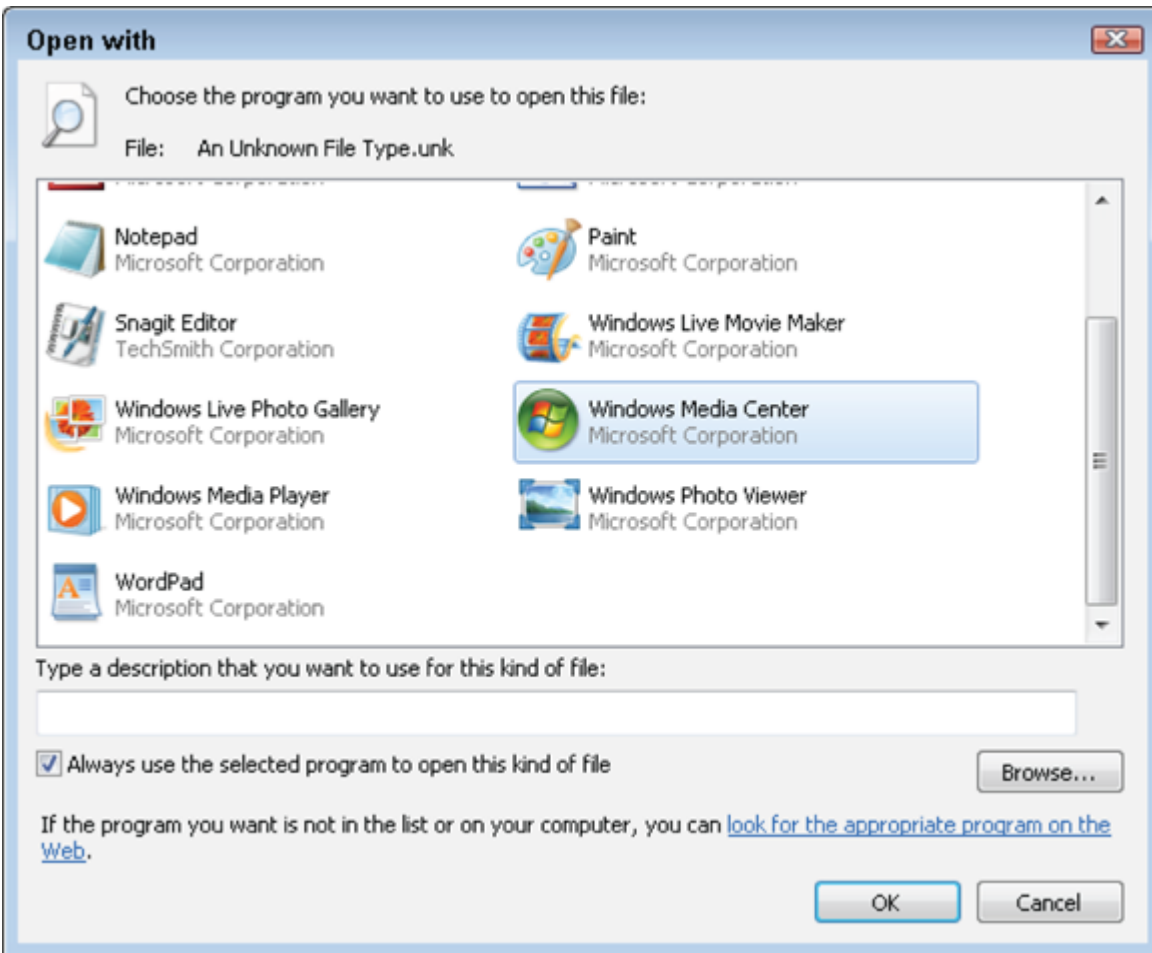
When working with Windows 7 or newer systems, you will not usually need to hold down the Shift key to reach the Open With options. Windows also displays a nested menu with recently chosen options for that file type, making it easier to switch between applications for that file type. Windows 10 replaced the nested menu with an easy-to-use dialog box, showing recently used or possible applications that may be used to open the file, or letting you go to the Microsoft Store to find an application.



**WARNING**

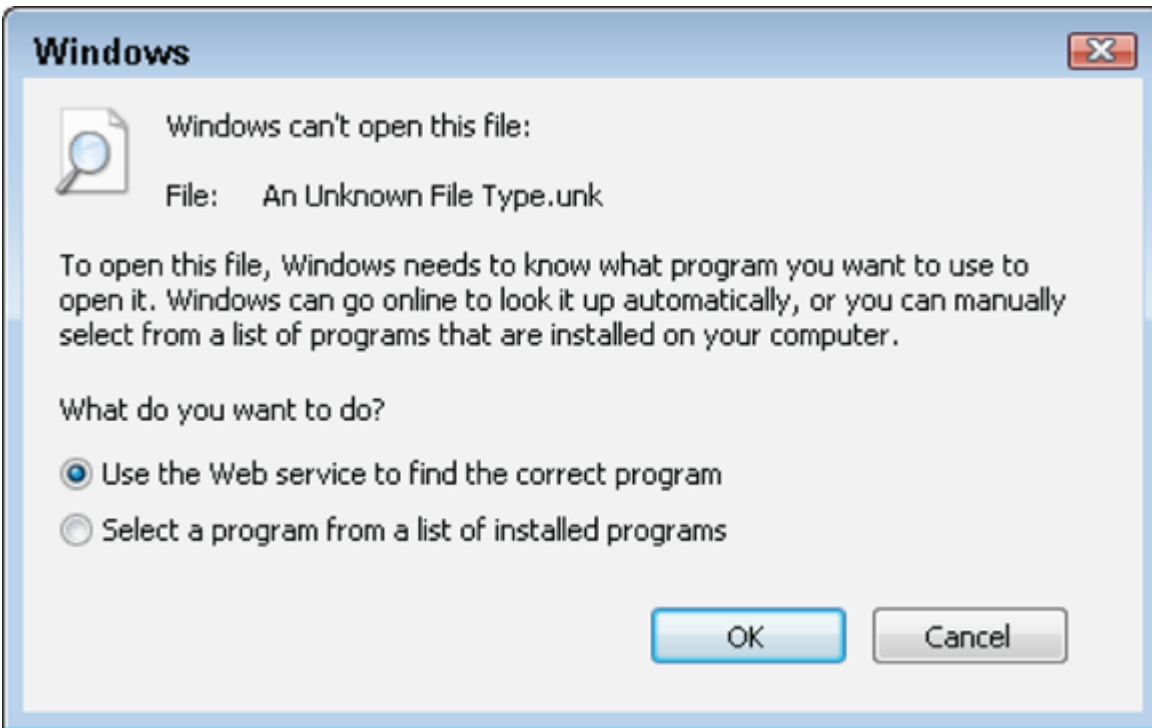
Microsoft does not recommend editing the Registry with the Registry editor to associate file types with applications since there are other methods available for this task. Using the Registry editor is required to change some Registry information. *If you make a mistake with the Registry, you might have to re-install the operating system.* For more information about editing the Registry with `regedit.exe` and `regedt32.exe`, consult Book 6, [Chapter 4](#).

For any files not currently associated with an application, you can double-click the file to open it. Windows checks its list of associations; if it cannot locate one, it prompts you for the name of the application that should be used, as shown in [Figure 4-2](#). This dialog box gives you the option to Always Use the Selected Program to Open This Kind of File, which, when selected, places an association with the file extension in the Registry. This is by far one of the easiest ways to create file associations.



**FIGURE 4-2:** You can create file associations in the Open With dialog box.

This process is easier when using Windows 7 and new systems, which also offers to check with Microsoft to see what program can be used with that file extension, in addition to letting you choose it manually, as shown in [Figure 4-3](#), while Windows 10 uses the same dialog box you saw with the Open With option.



**FIGURE 4-3:** Windows 7 offers to locate the application required to work with a file based on its extension.



**REMEMBER** If you are not sure which program you should use, clear the Always Use the Selected Program to Open This Kind of File or Always Use This App to Open .xyz Files check box (from the Open With dialog box; refer to [Figure 4-2](#)) prior to choosing the application you want to use with the file. The file will be opened by the application you chose, but the association will not be recorded in the Registry. So, if you chose the wrong application, you can just double-click the file and choose another application.

If you make a mistake or need to change the application that opens a file, you can easily do this through the shortcut menu.

1. **Select the file.**

If you don't do this, the Open With option might be missing.

2. **Right-click the icon.**

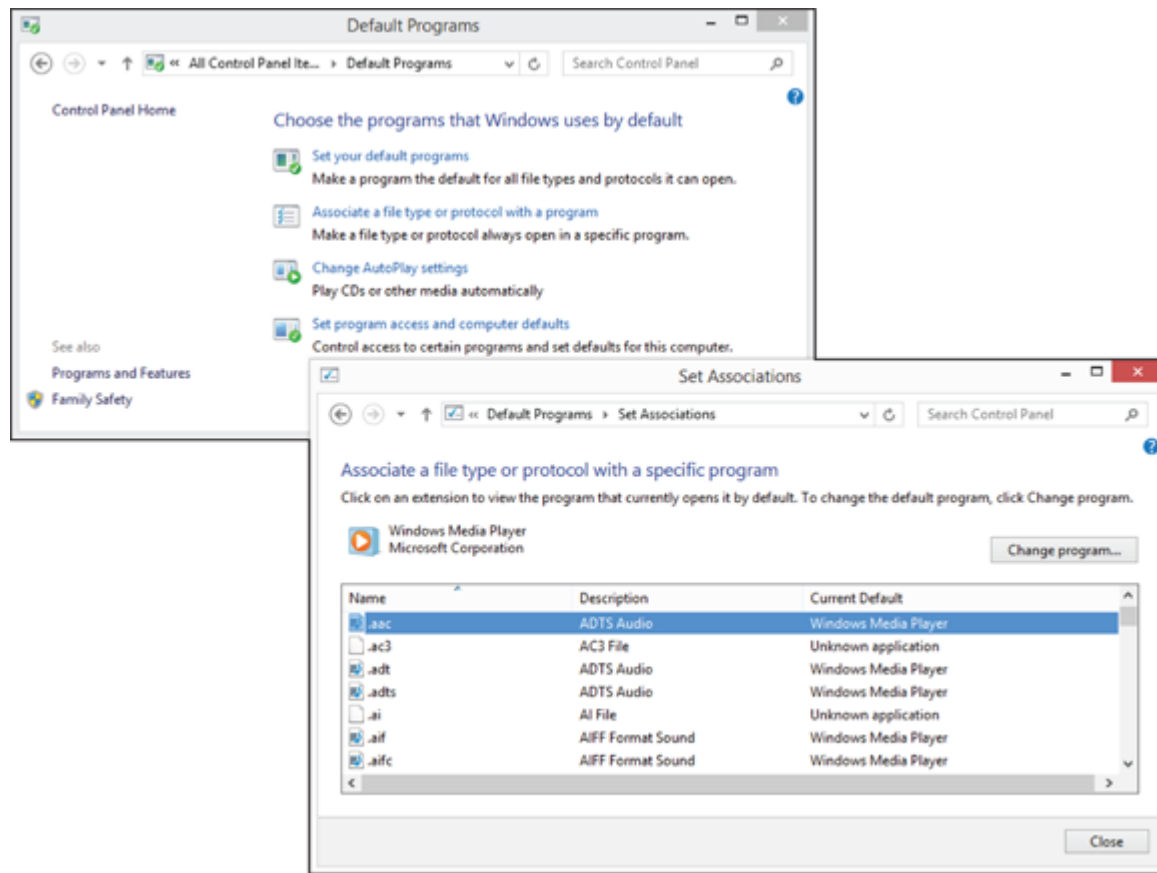
In the shortcut menu that appears, you should see an option for Open With. If more than one program can be used with the file type, Open With will be a nested menu listing your program choices, and you will also have the option to select Choose Default Program.



**REMEMBER** When you select Always Use the Selected Program to Open This Kind of File, you can associate the file extension with the application you select this time through the dialog box.

If you are looking for a few more options, or if you have made a mistake with your original file association, you can always use the Default Program Control Panel, which is shown in [Figure 4-4](#). To change an associated file using this method, use the following steps on a Windows 8.1 computer.

1. **Right-click the Start button and select Control Panel.**
2. **Click Default Programs.**
3. **Click Associate a File Type or Protocol with a Program.**
4. **Select the association you want to modify.**
5. **Click the Change Program button.**
6. **Select the new program you want to use to open this file type.**
7. **Click the Close button and close the Default Programs Control Panel.**

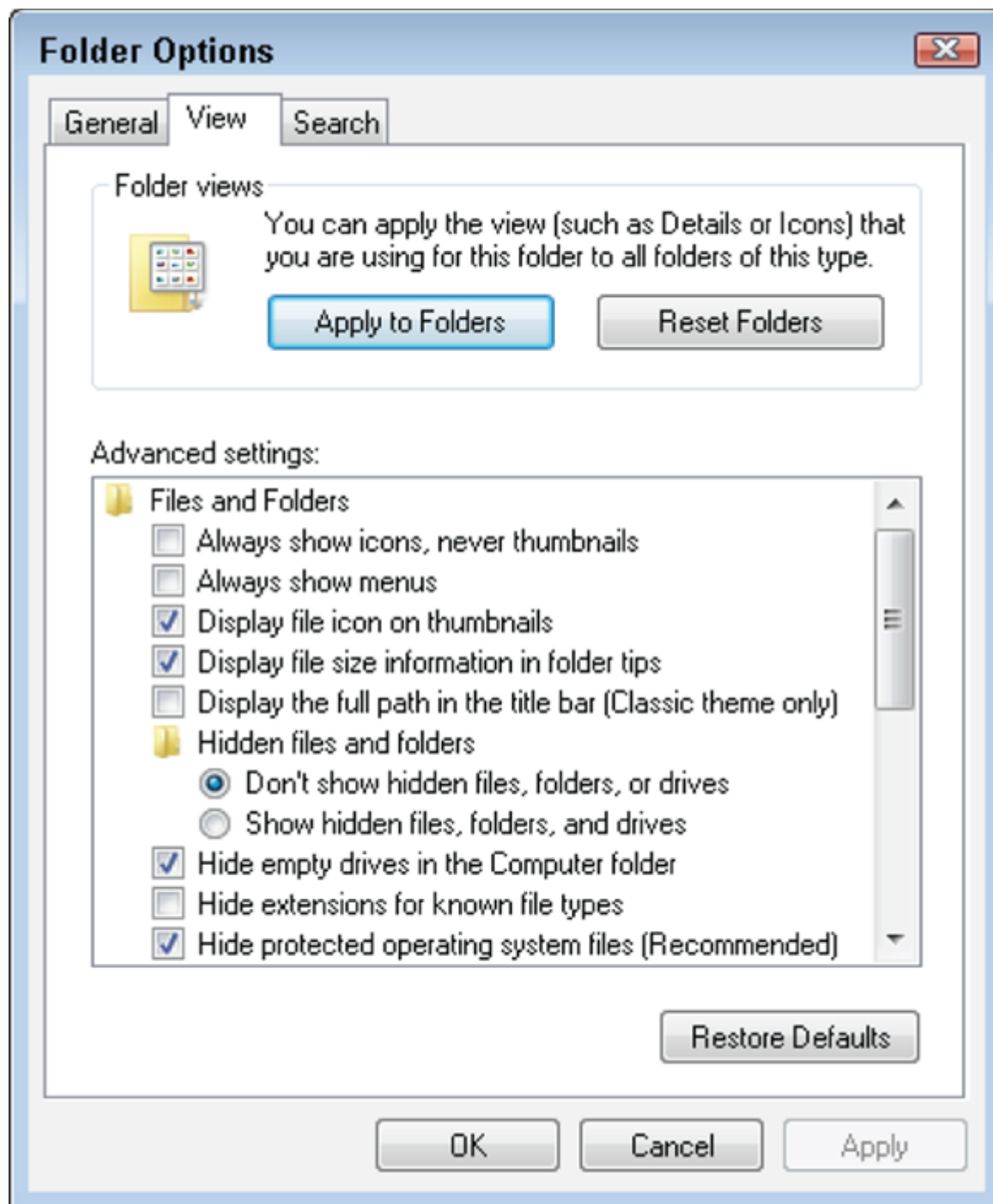


**FIGURE 4-4:** Changing the file type association using Default Programs on Windows 8.1.

## *Understanding file extensions*

In this section, I show you some of the major types of file extensions you can expect to see within your OS. By default, file extensions for registered file types are hidden. Registered files types are files that have extensions that already have applications associated with them. To display file extensions within Windows 7, follow these steps:

1. **Open any directory window, such as Computer.**
2. **Choose Organize ⇒ Folder and Search Options.**
3. **Click the View tab (shown in [Figure 4-5](#)).**
4. **Clear the Hide Extensions for Known File Types check box.**
5. **Click OK.**



**FIGURE 4-5:** You can tweak your Folder Options to display file extensions on your files.





TECHNICAL  
STUFF

Review the other settings on the View tab, as there are many you may find useful, including: Hidden Files and Folders ⇒ Show Hidden Files, Folders, and Drives and Hide Protected Operating System Files (Recommended). For more about hidden files and folders, see “[The basic attributes](#)” later in this chapter.

While you are taking a look at the Folder Options, review the items available on the General tab, which include:

- » **Open File Explorer to:** Choose Quick Access or This PC to have `Explorer.exe` open to show either the Quick Access item list or the contents of This PC.
- » **Browse Folders:** Controls how opening folders functions in `Explorer.exe`. You may choose to open each folder in the same window, or open each folder in its own window.
- » **Click items as follows:** Manages the display and clicking of folders and files to open them, which may be either a single-click or double-click to open an item.
- » **Privacy:** Controls what is retained in your Quick Access menu. You can choose between Show Recently Used Files in Quick Access or Show Frequently Used Folders in Quick Access. You also have an option to clear the File Explorer history.

In the sections that follow, I discuss common file extensions and how they are used on your computer.

## *Executables*

*Executable files* can perform tasks on the system. [Table 4-3](#) summarizes some of the file extensions common to executable files.

**[TABLE 4-3](#) Executable File Extensions**

<i>Extension</i>	<i>Type</i>	<i>Description</i>
------------------	-------------	--------------------

<b><i>Extension</i></b>	<b><i>Type</i></b>	<b><i>Description</i></b>
.bat	Batch file	A series of commands sequentially typed into a text file
.cmd	command file	Same as batch file
.com	MS-DOS command file	Program file, usually execute with only a command shell interface
.exe	Command line or graphical program	The most common extension for executable files
.ps1	PowerShell script file	Not executable themselves but require <code>powershell.exe</code> to be executed; they should be considered to be super batch files
.vbs	Visual Basic Script file	Not executable themselves but require either <code>wscript.exe</code> or <code>cscript.exe</code> to be executed; a cross between Visual Basic applications and batch files

### ***Major Office applications***

You need to be familiar with the file extensions associated with a few of the most popular office applications on the market. Some of these extensions are listed in [Table 4-4](#).

**TABLE 4-4 Application File Extensions**

<b><i>Extension</i></b>	<b><i>Type</i></b>	<b><i>Description</i></b>
.doc .docx	Document files	Usually associated with Microsoft Word; .doc is sometimes used by installations of WordPerfect. Files extensions with an x at the end are used by Microsoft Office 2007.
.dot .dotx	Document templates	Document templates for Microsoft Word. <code>normal.dot</code> is the default template for new documents.
.ppt .pptx .pps .ppsx	Microsoft PowerPoint documents	.ppt files open in the PowerPoint interface and are immediately editable. .pps files, when you double-click them, open directly in PowerPoint Slide Show mode and close as soon as the slide show finishes.
.pdf	Adobe Portable Document Format files	Adobe .pdf files are the de facto standard for document exchange when the targeted user's systems are unknown.

<i><b>Extension</b></i>	<i><b>Type</b></i>	<i><b>Description</b></i>
.xls .xlsx	Microsoft Excel document	Spreadsheets associated with Microsoft Excel.

### ***Compression utilities***

Over the years, and across operating systems, file compression has always been an issue, leading to the creation of numerous different compression formats. [Table 4-5](#) lists some of the common extensions for compressed files and where they are used. Although some utilities are based in one OS or another, today you can find compression and decompression tools for most formats in most operating systems.

**TABLE 4-5 Compression File Extensions**

<i><b>Extension</b></i>	<i><b>Type</b></i>	<i><b>Description</b></i>
.ace	Ace or WinAce	A high-compression format
.arc	Arc or Archive	Traditional Linux and Unix utility
.arj	Archiver Robert Jung (the creator of the format)	Traditional archive utility for MS-DOS
.bhx .hqx	BinHex files	Mac encoding format
.cab	Cabinet file	Microsoft format for distributing software
.rar	Roshal Archive (created by Eugene Roshal)	High-compression format used on most operating systems
.sit	Stuffit	Most popular Mac compression format
.tar	Tape archive files	Traditional, highly used archive format for Linux and Unix that can back up directory structures into a single file rather than compress them; often used in conjunction with <code>gzip</code>
.tgz	tar-gzip	Traditional, highly used compression format for Linux and Unix; actually a gzip-ed TAR file

<i><b>Extension</b></i>	<i><b>Type</b></i>	<i><b>Description</b></i>
.uu .uue	Uuencode	One of the most popular encoding algorithms for Linux and Unix
.zip	PKZIP	The grandfather of PC compression formats; still the most used format for the Windows world

## ***System files***

Several types of files drive your computer's operating system. Some of the extensions you should expect to see on system files are listed in [Table 4-6](#).

**TABLE 4-6 System File Extensions**

<i><b>Extension</b></i>	<i><b>Type</b></i>	<i><b>Description</b></i>
.bak	Backup files	Used as a default extension by a number of applications
.cpl	Control Panel files	Contains interface to adjust Windows settings
.dat	Data files	Used with the Registry files, such as <code>ntuser.dat</code>
.dll	Dynamic Link Library	Contains common and reusable code that can be called by any application to reduce the amount of code that has to be placed within specific applications
.ini	Initialization files	Text files that contain settings for applications; phased out in favor of the Registry
.msc	Microsoft Console settings files	Seen often with Windows 2000 or later and a bit with Windows NT 4.0
.msg	Error message files	Contains messages to be displayed in the event of an error; were used with the MS-DOS network client, and were only required if you wanted to see a text description of error codes
.msi	Microsoft Installer files	A file format used to distribute software to computers running the Windows Installer service

<b><i>Extension</i></b>	<b><i>Type</i></b>	<b><i>Description</i></b>
.ttf	True Type font definition files	Contains formula description used to display scalable fonts
.vxd	Virtual device drivers	Holds binary code for Windows-based device drivers

## ***Graphic files***

Graphics have been an important part of computers since computers were invented and were able to print. Early graphics were generated using the standard ASCII character set and used to create simple graphs or rudimentary graphics. A number of different formats have become popular; with the popularity of the Internet, the number of major graphic formats has greatly increased. For a listing of graphic formats, see [Table 4-7](#).

**TABLE 4-7 Graphic File Extensions**

<b><i>Extension</i></b>	<b><i>Type</i></b>	<b><i>Description</i></b>
.bmp	Bitmap	Used by MS Paint
.eps	(Adobe) Encapsulated PostScript	Used by several major graphics applications
.gif	Graphic Interchange Format	Owned by AOL (originally owned by CompuServe); designed to minimize download times
.jpg .jpeg	Joint Photographic Experts Group	A compression format that discards data (“lossy”) thought to be invisible to the human eye
.svg	Scalable Vector Graphics	A free and open graphics file format for vector graphics
.pcx	PC Paintbrush	An early Windows graphic format

<b>Extension</b>	<b>Type</b>	<b>Description</b>
.pdf	(Adobe) Portable Document Format	Readable by Adobe Acrobat and Adobe Reader
.png	Portable Network Graphics	A free photo standard planned as a replacement for .gif and .jpeg because it supports all the benefits of both formats and uses a Zip type algorithm for compression
.tif .tiff	(Aldus) Tagged Image File Format	Used as a common interchange format between most graphics applications; very popular with photographic manipulators; supports LZW (Lempel-Ziv-Welch) compression format to reduce file sizes and is not lossy

### *Other file extensions*

[Table 4-8](#) has some other extensions that are worth noting.

## **TABLE 4-8** Miscellaneous File Extensions

<b>Extension</b>	<b>Type</b>	<b>Description</b>
.asp .aspx	Active Server Page Extended	Server-side scripted HTML files
.jsp	Java Server Page	
.php	PHP: Hypertext Preprocessor	
.cda	CD Audio	Stores audio data on audio CDs
.css	Cascading Style Sheet	Stores HTML-style data
.htm, .html	HyperText Markup Language	Stores data displayed on websites
.tmp	Temporary file	A short-term storage file
.txt	Text file	ASCII text files that are readable on every operating system
.wav	Windows Audio files	Audio files designed specifically for use with Windows

Web servers use HTTP (HyperText Transfer Protocol) to send the information to your web browser. HTML is popular for displaying

information locally as well. Many vendors send Help files in this format so that they can be used on both their websites and as offline files.



FOR THE  
EXAM

You should be familiar with all these extensions and the categories to which they belong. Pay additional attention to executable, application, and system files.



ON THE  
WEB

Lab 4-1 provides some practice working with file associations. You will require a computer with Windows. The labs can be downloaded from the companion website at

[www.dummies.com/go/aplusaio](http://www.dummies.com/go/aplusaio).

## *Understanding File Attributes*

Since the first versions of MS-DOS and the FAT file system, files have had some basic attributes. The following sections deal with only the attributes that a computer user will manage: namely, Read-only, Hidden, System, and Archive. The discussion focuses on the basic attributes, the extended attributes offered by Windows NTFS, and how to change the file attributes.

### *How attributes are stored*

Attributes are stored as a single, 8-bit binary number. Because each bit can hold either a 0 or a 1, this yields 256 possible combinations of attributes — from eight 0s (no attributes applied; equal to 0 in decimal notation) to eight 1s (all attributes applied; equal to 255 in decimal notation).

Because each attribute holds a specific bit position, if several attributes are applied to a file, you can add the values (either binary or decimal) together to get a unique number that is 255 (11111111 in binary) or less for

each unique combination of attributes. For example, if the file had the attributes of Read-only (1), System (4), and Archive (32), the value of the attribute byte would be 1 + 4 + 32, or 37. Only 37 (00100101 in binary) could represent a file with these attributes. The full list of attributes is listed in [Table 4-9](#).

**TABLE 4-9** File Attributes

<i>Bit Position</i>	<i>Decimal Value</i>	<i>Binary Value</i>	<i>Attribute</i>
1	1	00000001	Read-only
2	2	00000010	Hidden
3	4	00000100	System
4	8	00001000	Volume Label
5	16	00010000	Sub-directory
6	32	00100000	Archive
7	64	01000000	Unused
8	128	10000000	Unused



**FOR THE  
EXAM**

For the A+ exams, you will be asked only about the Read-only, Hidden, System, and Archive attributes. Still, you should be aware of the Volume Label and Sub-directory attributes for real-world applications. You do not need to know the bit values of any of the attributes; just know what the four basic attributes are used for.

### *The basic attributes*

All files on your computer, regardless of your Microsoft OS or file system, have these four basic attributes:

- » Read-only
- » Hidden
- » System



## WORKING WITH THE VOLUME LABEL

In addition to these four basic attributes, one more attribute — Volume — is usually set on your hard drive. The Volume attribute is usually applied to only one directory entry per drive (excluding the directory entries that are used for long filename entries) and stores the volume label for the drive. This is the name that appears with the drive when you look at the drives in Computer or My PC, so naming it appropriately will make it easier to keep straight what is found on each drive.

The directory entry that contains the label can be modified through one of the following methods:

- Enter the `label` command at a command prompt.
- Edit the Label field in the Properties window of your drive.
- Use the `Rename` command in the Computer (or My PC for Windows 8.1 users or This PC for Windows 10 users) window.

Descriptions of the four common attributes are listed in [Table 4-10](#).

**TABLE 4-10 Basic File Attributes**

<i>Attribute</i>	<i>Description</i>
Read-only	Cannot be deleted from the command line and cannot be written to or saved over.
Hidden	Invisible to users unless those users have changed their viewing options to display hidden files. Hidden files cannot have their attributes changed by the <code>attrib.exe</code> command.
System	Flagged as being required by the operating system. They cannot have their attributes changed by the <code>attrib.exe</code> command.
Archive	Ready for archiving or backing up. This attribute is used by some backup programs so that they can perform incremental backups. Currently, the <code>xcopy</code> and <code>robocopy</code> commands support the <code>/a</code> and <code>/m</code> switches, indicating that only files that have the Archive attribute set should be copied, while <code>/m</code> also clears the Archive attribute. When the file is modified, the Archive attribute will automatically be reset on it.

Any time files are modified, the Archive attribute is automatically set. Thus, after Windows is installed, all files have the Archive attribute enabled. Windows also sets Read-only, Hidden, and System attributes on many required system files to prevent accidental modification or deletion by the user. Other than these files, though, the only attribute automatically set is Archive. You can see how to manually set these attributes later in the upcoming section, “[Setting basic attributes](#).”

## ***Windows NTFS extended attributes***

Windows has three other file attributes that are used on NTFS partitions. These three attributes are often referred to as *extended attributes*:

- » **Compress:** Used to enable on-the-fly file level compression of data
- » **Encrypt:** Used to enable on-the-fly file level encryption of data
- » **Index:** Used to allow files to be indexed by the OS Indexing Service

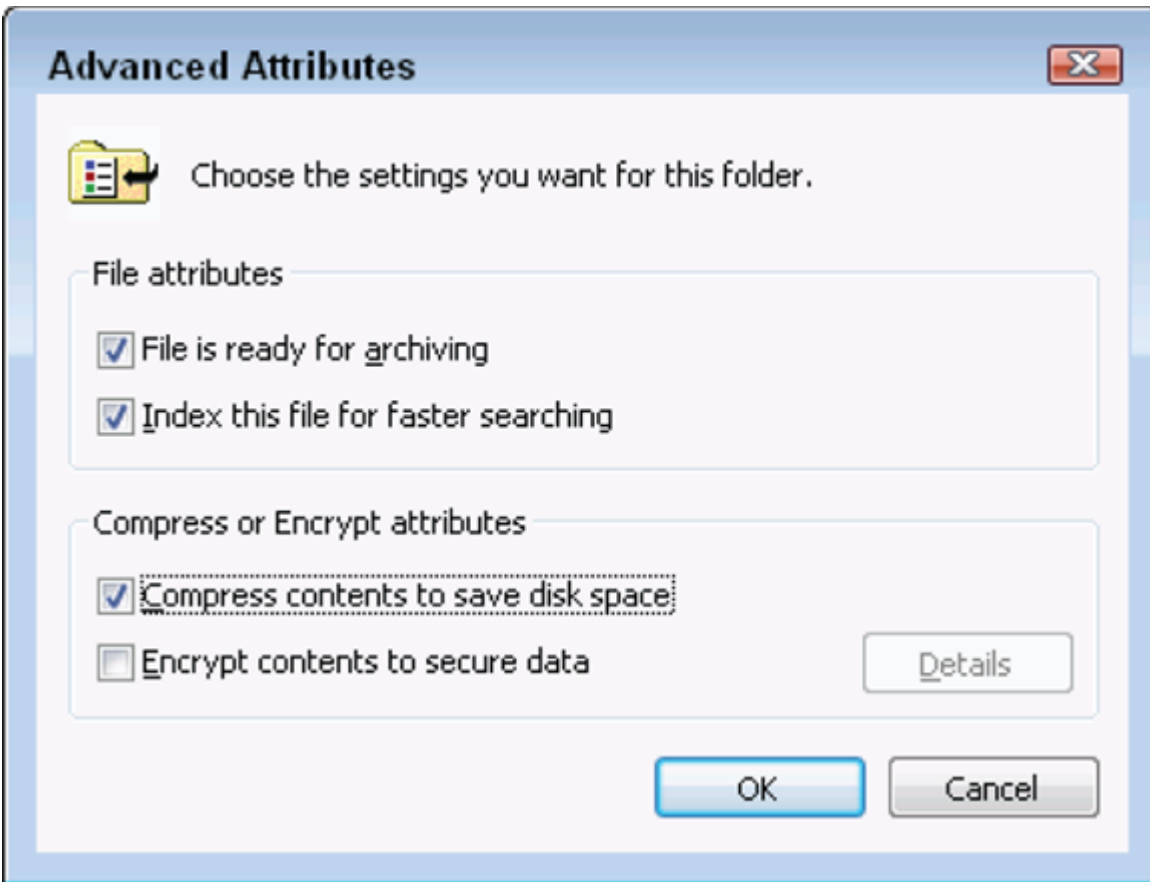
The sections that follow take a closer look at each of these attributes.

To view compressed and encrypted files in Windows Explorer in a different color, use the View settings in Folder Options, and select the check box for Show Encrypted or Compressed NTFS Files in Color. This option will show compressed files in blue and encrypted files in green. Files can only be compressed or encrypted, but not both. Keep reading to find out more about these options.

### ***Compress***

The Compress attribute allows and restricts file compression. To compress a file or folder, follow these steps:

1. **Right-click the file or folder and choose Properties.**
2. **In the Properties dialog box that appears, click the Advanced button.**
3. **From the Advanced Attributes dialog box, you can compress the file or folder by selecting the Compress Contents to Save Disk Space check box, as shown in [Figure 4-6](#).**



**FIGURE 4-6:** The Compress attribute is set on a file-by-file or folder basis.

If you are using the default Windows Explorer settings prior to Windows 10, files and folders that have the Compress attribute set will be displayed with blue text. Windows 10 defaults to not showing these files in blue.



**TECHNICAL  
STUFF**

The file compression algorithm used is Lempel-Ziv compression, which is a lossless compression method. If the file you are compressing is greater than 30GB, compression may fail.

To compress a file, the file needs to be read into memory, where compression takes place, and then rewritten to the disk in its compressed form. When you change the Compress file attribute, the OS saves the change to the attribute prior to actually going to steps of compressing the

file. This is done in two steps because the attributes are stored in the MFT and not in the actual file itself. After the attribute change is recorded, file compression for that file is performed. Because of the small chance that something could go wrong during the compression phase, some of the files on your hard drive might have the Compress attribute set, yet not actually be compressed. One situation that might cause this inconsistent Compress attribute is a power interruption during the compression process, resulting in the attribute change being made but a compressed version of the file not saved. To ensure that this has not happened, you could use the `compact.exe` command line utility.

You can use `compact.exe` to compress or decompress files from the command line. It supports switches that allow it to process sub-directories as well. If you suspect inconsistent compression states for your files, you can use the `/F` (force switch), which goes through the process of compressing all files, even if they already have the Compress attribute. This does not double-compress files, but rather ensures that all files that are supposed to be compressed actually are compressed. See [Table 4-11](#) for a complete list of the switches that `compact.exe` makes use of. If you run `compact.exe` without any switches, it will display compression information for the files in your current directory.

**TABLE 4-11** `compact.exe` Command Switches

<i>Switch</i>	<i>Description</i>
<code>/A</code>	Displays files with the hidden or system attributes. These files are omitted by default.
<code>/C</code>	Compresses the specified files. Directories will be marked so that files added afterward will be compressed.
<code>/F</code>	Forces the compress operation on all specified files, even those which are already compressed. Already-compressed files are skipped by default.
<code>/I</code>	Continues performing the specified operation even after errors have occurred. By default, <code>compact.exe</code> stops when an error is encountered.
<code>/Q</code>	Reports only the most essential information.
<code>/S</code>	Performs the specified operation on files in the given directory and all sub-directories. Default directory is the current directory.

---

Switch	Description
--------	-------------

---

/U

Uncompresses the specified files. Directories will be marked so that files added afterward will not be compressed.

---



FOR THE  
EXAM

If you move a compressed file within a partition, the file will retain its Compression attribute. However, if you copy a compressed file to a folder, it inherits the Compression attribute that is set for the destination folder.

## Encrypt

An *encrypted* file is protected only against being read. This means that the file can be moved to another location on the same partition or renamed; these actions require modifying the directory table and do not constitute reading the file. The file may also be deleted if the appropriate NTFS permissions have not been applied to it.

To encrypt a file or folder, follow these steps:

1. **Right-click the file or folder and choose Properties.**
2. **In the Properties dialog box that appears, click the Advanced button.**
3. **From the Advanced Attributes dialog box, you can encrypt the file or folder by selecting the Encrypt Contents to Secure Data check box.**

If you are using the default Windows Explorer settings prior to Windows 10, files and folders that have the Encrypt attribute set will be displayed with green text. Windows 10 does not show these files in green.



FOR THE  
EXAM

If the user who encrypted the file then moves or copies a file between NTFS partitions (even between computers), the file will

remain encrypted. This is different from Compression or NTFS permissions. If the file is copied to a non-NTFS partition, the file is automatically decrypted. If you cannot decrypt the file, you will receive an Access Denied message when you attempt to move the files to a location that is on a different partition.



TECHNICAL  
STUFF

Public Key Infrastructure (PKI) is a system that allows for authentication users and encryption of data. PKI works with key pairs that are used to encrypt or decrypt data. The pair of keys is defined as *private* (known only to the user) or *public* (known to all other users of the infrastructure). Public keys are usually stored in certificates. When data is encrypted by using a public key, it can be decrypted only by using the related private key from the key pair. Encrypting File System (EFS) makes use of PKI. If you do not have an infrastructure, the local workstation will auto-generate keys on the local computer to support EFS. If you are using EFS within an organization, you should make use of an enterprise-wide PKI, which can be implemented by using the Microsoft Windows Active Directory Certificate Services.

Windows does not allow you to both encrypt and compress a file. This is because compression requires that the file be rewritten, and encryption does not allow the file to be rewritten. The reason why encryption does not allow the file to be rewritten is because the file header contains the file's encryption keys. These keys are protected by the public key of the user who encrypted the file as well as the public key of the EFS Recovery Agents. The EFS Recovery Agent is specified in the local public key policies of the computer or in Active Directory. By default, on a workstation or an Active Directory domain, the EFS Recovery Agent will be set to the Administrator account. When a file is encrypted, the only people who can read the file are the user who enabled encryption, the EFS Recovery Agent, and any other users who specifically had their public keys used to encrypt the file's encryption keys.

To allow other people to access your encrypted files, follow these steps for a file that has already been encrypted:

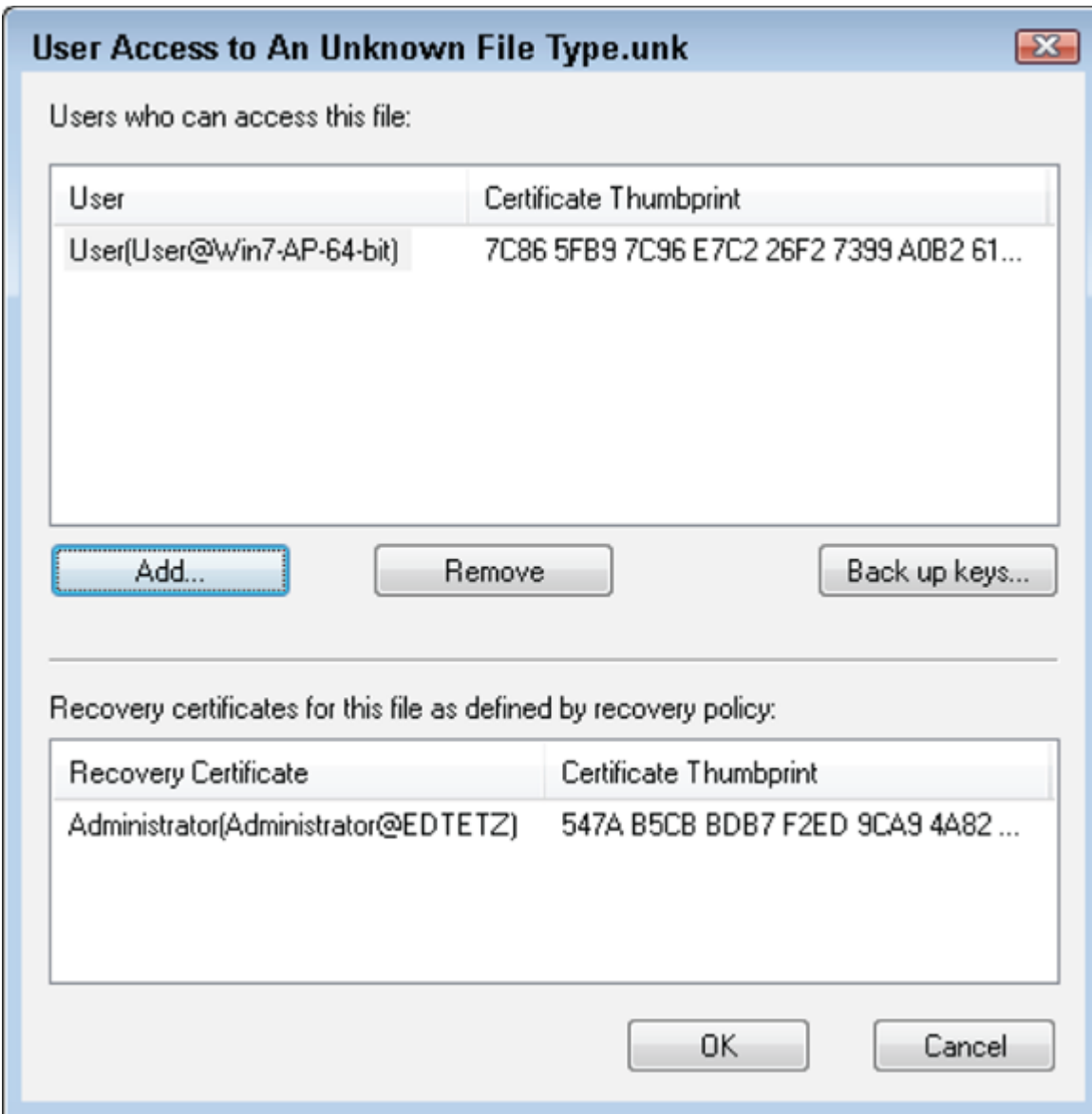
1. **Right-click the file or folder and choose Properties.**
2. **In the Properties dialog box, click the Advanced button.**
3. **In the Advanced Attributes dialog box, click the Details button.**

The Encryption Details for the file dialog box opens, listing all users who can transparently access the file.

4. **Click the Add button.**

The Select User dialog box opens.

5. **If the user you want to grant access to is not on the list, your action depends on whether you are in a domain:**
  - *If you are in a domain*, click the Find User button to access the standard OS Select User dialog box.
  - *If you are not in a domain*, select the user you want to add and then click OK, as shown in [Figure 4-7](#).
6. ***If you are not in a domain or if the user you want to grant access to is not in the domain***, you will need to get him to send you a copy of his certificate, which you will import into the system by double-clicking the certificate file in Windows Explorer.
7. **Click OK on each of the other dialogs that opened.**



**FIGURE 4-7:** You can grant other users access to your encrypted files.

If you do not have an enterprise PKI, you cannot access certificates for other users, so you will not be able to easily grant other users access to encrypted files.



**REMEMBER** Similar to `compress.exe` for compressing files, you can use the command line utility `cipher.exe` to encrypt files from the command line or in batch files.



In the same way that you could use `compress.exe` for compressed files, you can use `cipher.exe` for encrypted files. [Table 4-12](#) reviews some of the switches that can be used with the `cipher.exe` command.

**TABLE 4-12** `cipher.exe` Command Switches

Switch	Description
/D	Decrypts the specified files or directories. Directories will be marked so that files added afterward will not be encrypted.
/E	Encrypts the specified files or directories. Directories will be marked so that files added afterward will be encrypted.
/H	Displays files with the hidden or system attributes. These files are omitted by default.
/B	Stops performing the specified operation if errors have occurred. By default, <code>cipher.exe</code> continues when errors are encountered.
/K	Creates new file encryption key for the user running <code>cipher.exe</code> . If this option is chosen, all the other options will be ignored.
/Q	Reports only the most essential information.
/R	Generates an EFS recovery agent key and certificate, then writes them to a PFX file (containing certificate and private key) and a CER file (containing only the certificate). An administrator may add the contents of the CER to the EFS recovery policy to create the recovery agent for users, and import the PFX to recover individual files.
/S	Performs the specified operation on directories in the given directory and all sub-directories.
/U	Tries to touch all the encrypted files on local drives. This will update the user's file encryption key or the recovery agent's key to the current ones if they are changed. This option does not work with other options except /N.
/W	Removes data from available unused disk space on the entire volume. If this option is chosen, all other options are ignored. The directory specified can be anywhere in a local volume. If it is a mount point or points to a directory in another volume, the data on that volume will be removed.
/X	Backup EFS certificate and keys into file filename. If <code>efsfile</code> is provided, the current user's certificate(s) used to encrypt the file will be backed up. Otherwise, the user's current EFS certificate and keys will be backed up.

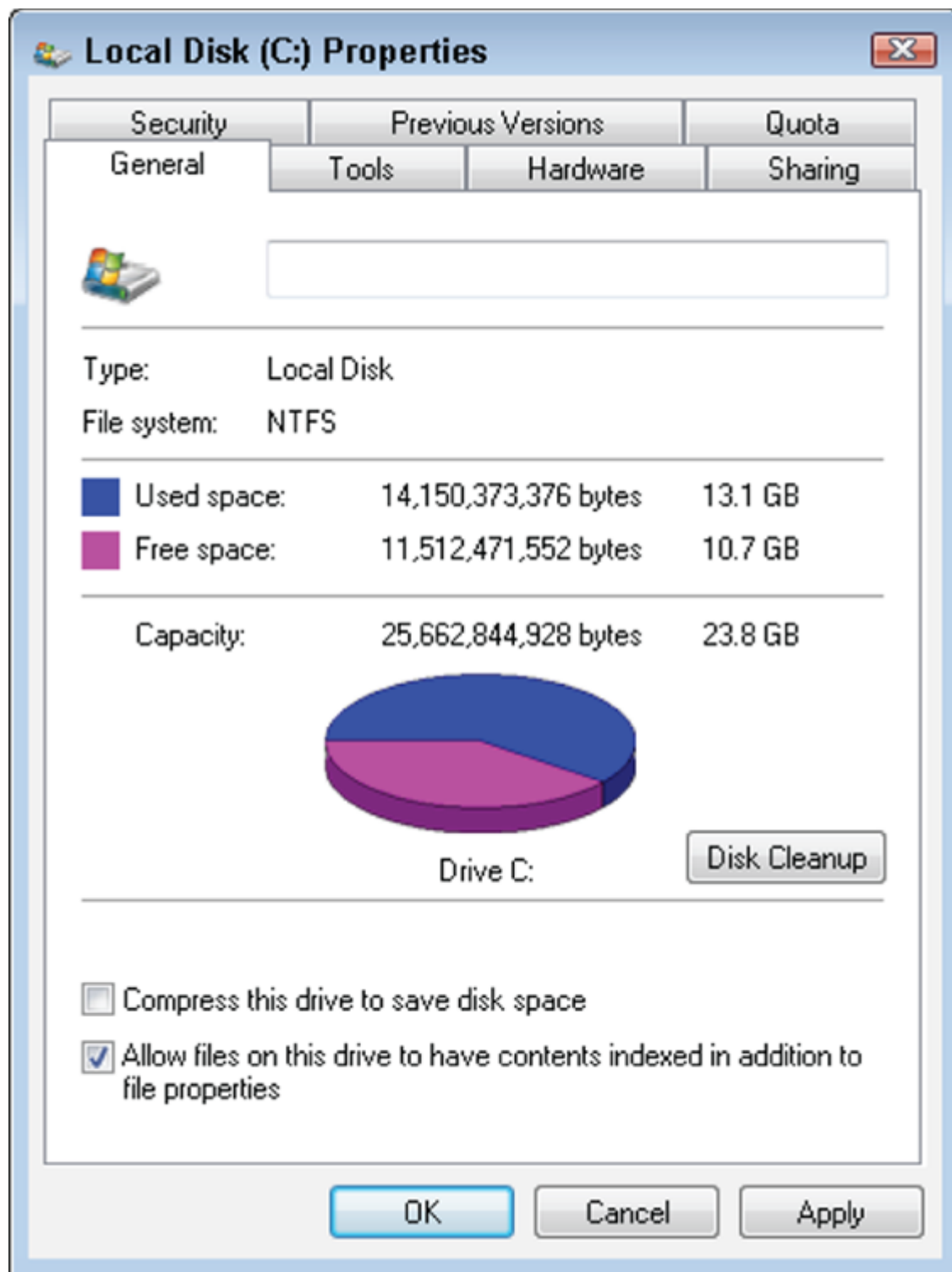
## Index

Indexing the file system will greatly improve the time it takes to search your hard drive. On the downside, though, indexing demands space on your drive. Indexing not only records the filenames and locations, but will also record words found in your files. The indexing service has a set of “noise words” that it ignores, such as *it*, *that*, *is*, *not*, and *the*. As files are indexed, the results are stored in a catalog; when searching for files, you can specify the catalog you want to use. By default, a catalog — a system — is configured to index your local files on your hard drives. Find this default catalog in the System Volume Information directory of your boot drive or c: drive.

To enable basic indexing of your drive, follow these steps:

1. **Right-click your drive in Computer (or My PC for Windows 8.1 users) and choose Properties.**
2. **Select the Allow Files on This Drive to Have Contents Indexed in Addition to File Properties check box (see [Figure 4-8](#)).**

This enables indexing, provided that the Indexing Service is running.



**FIGURE 4-8:** Indexing can be enabled for your whole drive or for just a folder.

You can verify that the Indexing Service (named Windows Search since Windows 7) is running by using the Services Administrative Tool (select

Start and type **Services.msc**) and verifying that the Windows Search is started. Windows will always have the Windows Search Service running.

Just because a folder is allowed to be indexed, that does not mean that it will be indexed. Windows includes a default set of locations that it will index for you, which you are able to modify or add to. Although you may search the Control Panel for Indexing Options, the most likely way you will get to this dialog is when you are attempting to search nonindexed locations. To see this in action, follow these steps on Windows 7:

**1. Open a folder in Windows Explorer that is not indexed.**



**TIP**

This is just about all folders on the root of the C: drive, or folders on other drives on your computer.

**2. Type a search word into the Search field in the upper-right corner of the window and press Enter.**

A gold band will be displayed in the window stating that Searches Might Be Slow in Non-indexed Locations: <Folder Location>. Choose Click to Add to Index, as shown in the background of [Figure 4-9](#).

**3. Click in the gold band to access options, which include Add to Index and Modify Index Locations.**

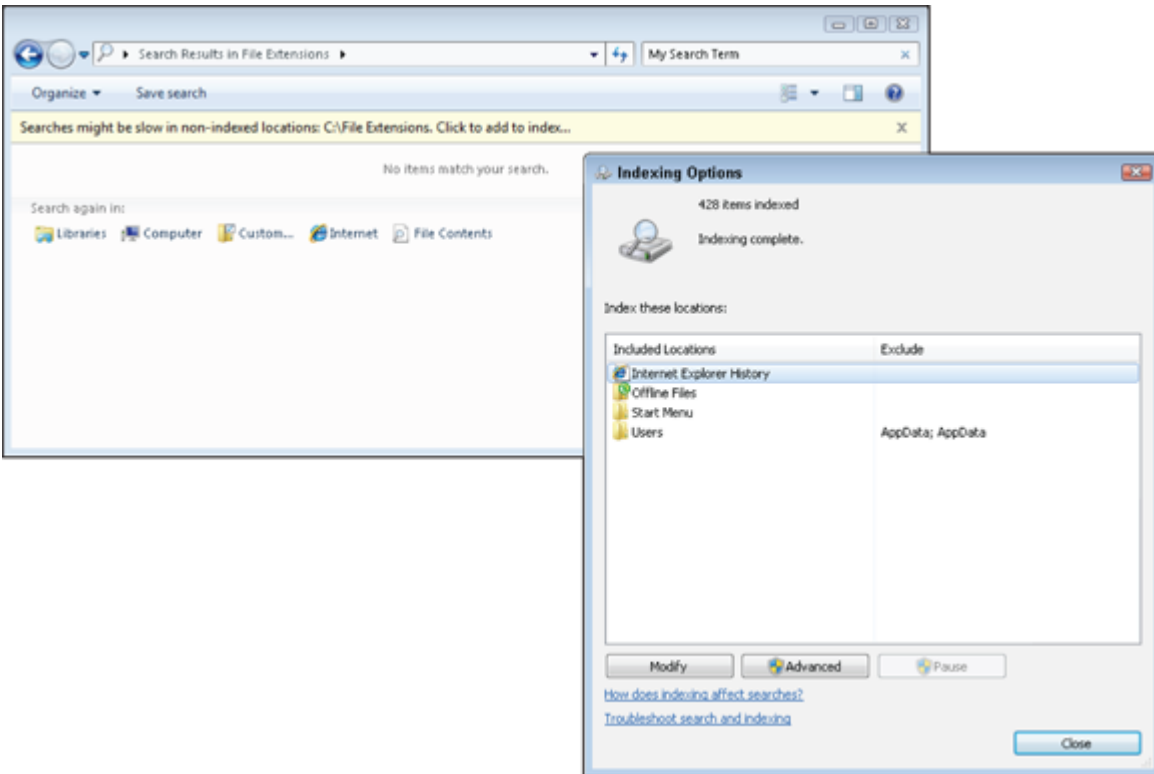
**4. To add the currently nonindexed location to your index:**

- a. Choose Add to Index.
- b. Confirm your choice by clicking the Add to Index button in the Add to Index dialog.

**5. For each location you want to *modify* in your index:**

- a. Choose Modify Index Locations to open the Indexing Options dialog, shown in the foreground of [Figure 4-9](#).
- b. Click the Modify button. This will open the Indexed Location dialog.

- c. Place check marks in front of any folders you want to have indexed.



**FIGURE 4-9:** You must have folders included in the index to be able to search by the index.

When using Windows 10 getting to Indexing Options becomes easier. When you click in the Search field in the top right corner of File Explorer, you will see the Search Tools Ribbon at the top of your screen. Select Search ⇒ Advanced Options ⇒ Change Index Locations; this will open the Indexing Options dialog which allows you to adjust the locations on your computer which are indexed.

## *Setting basic attributes*

Like so many other areas of an operating system, where there are many different ways to achieve your goal, there are many different ways to change the attributes of files. The first method — using the command line — is the only way common to all Microsoft OSes, but keep reading to see how to set attributes via the Windows GUI.

## *Command line*

To change file attributes from the command line, start at the Command Prompt window. (For Windows 7, choose Start ⇒ All Programs ⇒ Accessories, right-click Command Prompt, and choose Run as Administrator. For Windows 8.1 and Windows 10, choose Start, type **cmd**, right-click and select Command Prompt from the search results, and choose Run as Administrator.) In the Command Prompt window, you can set attributes by using the `attrib.exe` command. The basic syntax for the command is this:

```
attrib <attribute to set (H, S, R, A)> <files to modify>
```

Setting attributes also includes a plus sign (+; enabled) or minus sign (-; disabled), followed by a one-letter code for each attribute. For example, to set the read-only attribute and remove the archive attribute from the `C:\Windows\notepad.exe` file, use the following:

```
attrib.exe +R -A C:\Windows\notepad.exe
```

The one-letter codes are as follows:

- » A: Archive
- » H: Hidden
- » R: Read-only
- » S: System



**REMEMBER** Windows includes an `I` attribute for Indexed, or more correctly, Not Indexed. Setting this attribute is the same as deselecting the Allow This File to Have Contents Indexed in Addition to File Properties check box in the Advanced Attributes dialog of the file, which is discussed earlier in this chapter in the “[Index](#)” section. Because indexing has already been covered, this section deals with the four remaining attributes.

If you use the `attrib` command without any options, it displays a list of current attributes of all files in the current directory. Here is a sample of what that would look like:

```
C:\>attrib.exe
A SHR C:\bootmgr
A SH C:\BOOTNXT
A SH C:\pagefile.sys
A SH C:\swapfile.sys
```

If you use the `attrib.exe` command with options but without specifying a filename, you set the attribute(s) for all the files in the current directory. Here is an example of the command and the attributes that would be set:

```
C:\>attrib.exe -A -S -H -R
C:\bootmgr
C:\BOOTNXT
C:\pagefile.sys
C:\swapfile.sys
```

You can specify a file after the `attrib` command to see the current attributes of that file, or you can include the one-letter codes to set the attribute(s), like this example referencing `C:\boot.ini`:

```
C:\>attrib.exe C:\boot.ini
A C:\BOOT.INI
C:\>attrib.exe +h +r C:\boot.ini
C:\>attrib.exe C:\boot.ini
A HR C:\BOOT.INI
```

Another option you can include with the `attrib.exe` command is `/s`, which instructs `attrib.exe` to process the files in all sub-directories. This does not change the attribute on the sub-directories, just the files in the sub-directories. Using `/d` will change the attributes of the directories as well.

There are some restrictions on changing attributes with the `attrib.exe` command. Hidden and System files will not have their attributes changed unless the current Hidden or System attribute is also specified in a single command. Examine the following command sequence, which shows an example of dealing with Hidden or System files:

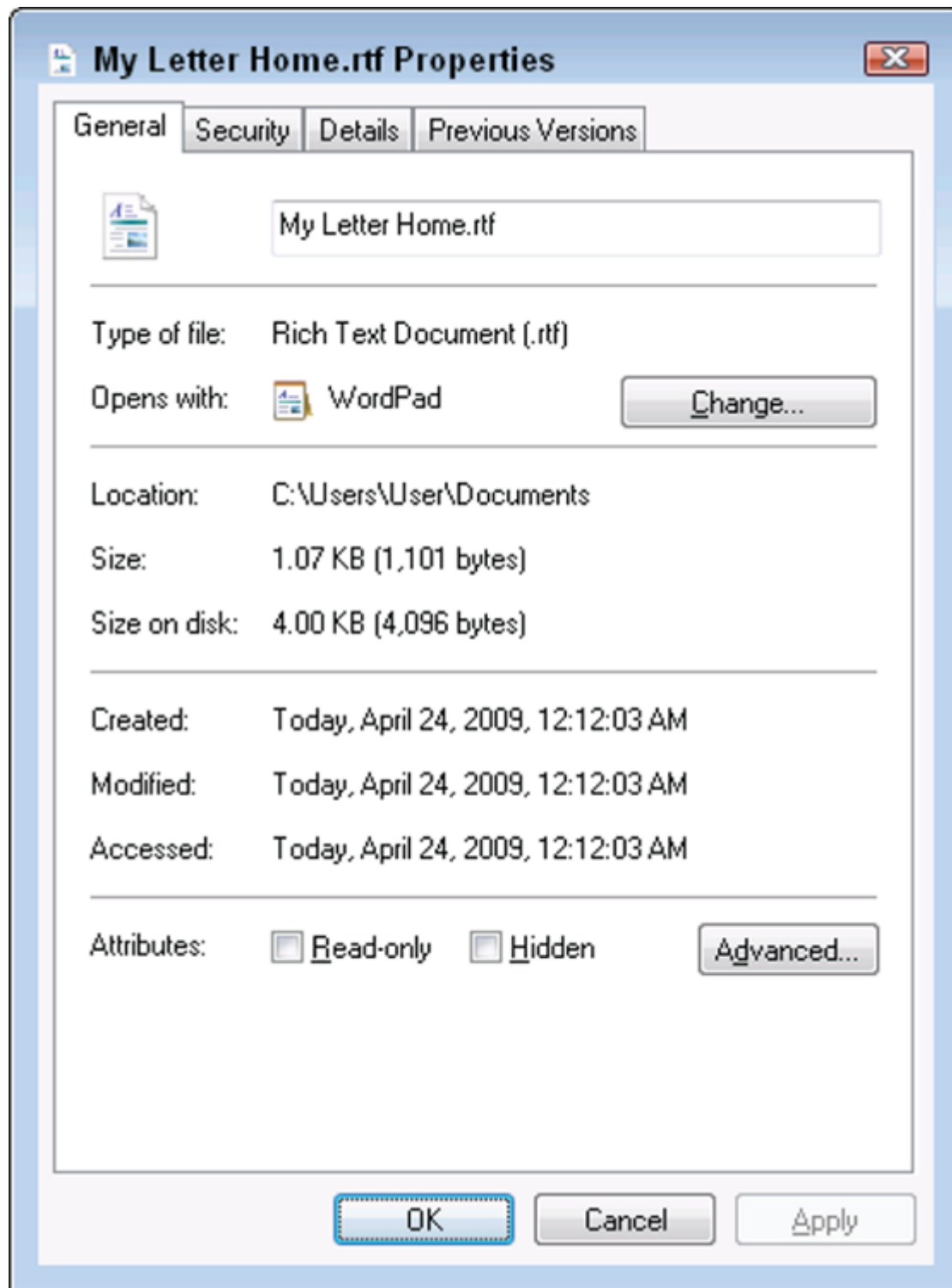
```
C:\>attrib.exe C:\boot.ini
A SH C:\boot.ini
C:\>attrib.exe -S -H -A -R C:\boot.ini
C:\>attrib.exe C:\boot.ini
```

```
C:\boot.ini
C:\>attrib.exe +S C:\boot.ini
C:\>attrib.exe +R C:\boot.ini
Not resetting system file - C:\boot.ini
C:\>attrib.exe C:\boot.ini
S C:\boot.ini
C:\>attrib.exe +R +S C:\boot.ini
C:\>attrib.exe C:\boot.ini
S R C:\boot.ini
C:\>attrib.exe +H C:\boot.ini
Not resetting system file - C:\boot.ini
C:\>attrib.exe +H +S C:\boot.ini
C:\>attrib.exe C:\boot.ini
SHR C:\boot.ini
C:\>attrib.exe +S +H -R C:\boot.ini
C:\>attrib.exe C:\boot.ini
C:\boot.ini
```

## ***Windows GUI***

In addition to the command line interface for changing attributes, Windows offers a GUI interface. When you right-click a file, you only see the options for Read-only, Hidden, and Archive when working with FAT 32 partitions. If you are working with NTFS partitions, the Archive check box is replaced with an Advanced button, as shown in [Figure 4-10](#).

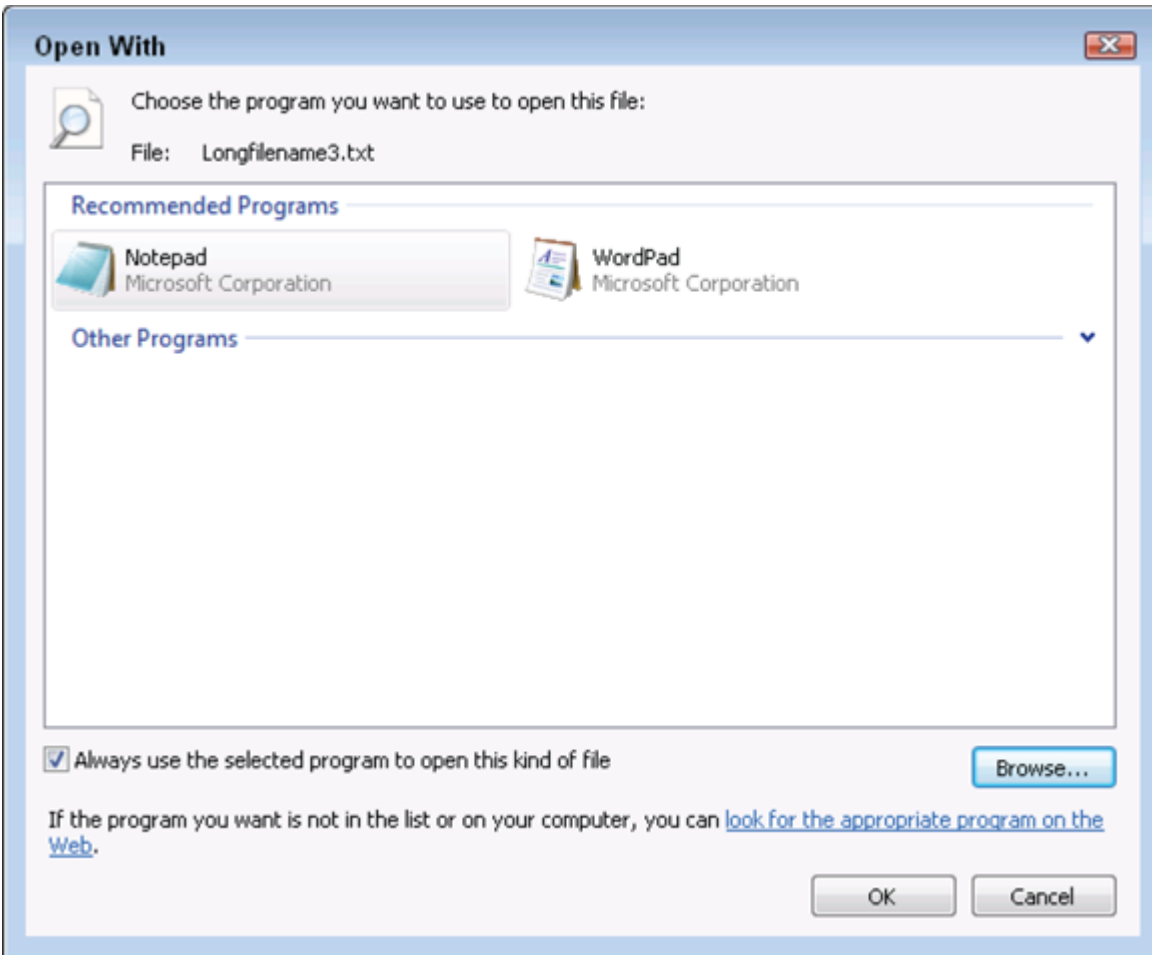




**FIGURE 4-10:** On NTFS partitions, you see only the Read-only and Hidden attributes.

Clicking the Advanced button allows you to set the Archive attribute as well as the Windows NTFS advanced attributes of Index, Compress, and

Encrypt. See [Figure 4-11](#).



**FIGURE 4-11:** The Advanced Attributes window is available only on NTFS partitions.



ON THE  
WEB

Lab 4-2 provides some practice working with attributes via the command line. For this exercise, you need a computer running Windows. The lab can be downloaded from the companion website at [www.dummies.com/go/aplusaio](http://www.dummies.com/go/aplusaio).

## Getting an A+

This chapter discusses file and directory management from the point of view of file-naming and file attributes. The following major points are

covered:

- » Windows supports simulated 8.3 naming for backward compatibility.
- » The four basic file attributes are Read-only, Hidden, System, and Archive.
- » Windows supports additional file attributes for compression, encryption, and indexing. These attributes are available only on the Windows NT File System (NTFS).
- » The Archive attribute is still used by many backup programs to locate files that have changed since the last backup.

## *Prep Test*

- 1. What is the maximum character length of a filename under Windows 7?**
  - (A) 64
  - (B) 128
  - (C) 254
  - (D) 255
  - (E) 256
  
- 2. You are moving several of Bob's files from a directory to another directory on the same partition. What message should you receive when you encounter an encrypted file?**
  - (A) You should not receive a message; the file will just be moved.
  - (B) You should get an Access Denied message.
  - (C) You should get a message stating that you could not read the file and that it may be corrupted.
  - (D) You should get a message stating that the file cannot be moved because it is encrypted.

**3. Which of the following can be used to associate file extensions with an application? Choose all that apply.**

- (A) `attrib.exe`
- (B) `cipher.exe`
- (C) Shift+right-click and choose Open With.
- (D) Choose Tools ⇒ Folder Options ⇒ View tab.

**4. Which of the following are extensions of executable files? Choose all that apply.**

- (A) `.ini`
- (B) `.prg`
- (C) `.exe`
- (D) `.cmd`

**5. Which of the following file extensions are associated with compression programs? Choose all that apply.**

- (A) `.com`
- (B) `.zip`
- (C) `.cmp`
- (D) `.cab`

**6. Which of the following attributes are associated with files on your hard drive? Choose all that apply.**

- (A) Restrict-Modify
- (B) Archive
- (C) Visible
- (D) Hidden

**7. When you copy an NTFS compressed file to a FAT32 partition, what happens to the file?**

- (A) The copy action is denied.

- (B) The file is copied but remains compressed, so it is unreadable.
- (C) The file is copied but becomes uncompressed.
- (D) The file can be copied only if the FAT32 partition has been compressed with DriveSpace compression.

## Answers

1. **D.** The maximum length of a filename is 255 characters. See “[Long and short filenames.](#)”
2. **A.** As long as the move is within one partition, the files will just be moved. If the directories are on different drives, you would receive an Access Denied message. Refer to “[Windows NTFS extended attributes.](#)”
3. **C.** `attrib.exe` is used to change file attributes and not file associations. `cipher.exe` is used to change file encryption settings, and the View tab does not contain options for changing file associations. Peruse “[Creating file associations.](#)”
4. **C, D.** `.exe` files are executable program files and `.cmd` files are text files similar to batch files but are treated as executable. Take a look at “[Understanding file extensions.](#)”
5. **B, D.** PKZIP files use the `.zip` extension, and `.cab` files are a proprietary, Microsoft compression format. Peek at “[Understanding file extensions.](#)”
6. **B, D.** The four basic attributes are Read-only, Hidden, System, and Archive. The advanced NTFS attributes are Compress, Encrypt, and Index. Look over “[Understanding File Attributes.](#)”
7. **C.** Compressed files copied from NTFS volumes to any other type of disk will become uncompressed. If they are copied to other NTFS volumes, they will inherit the compression attribute from the destination folder. Study “[Windows NTFS extended attributes.](#)”

# Chapter 5

## Command Prompt Procedures

---

### IN THIS CHAPTER

- » Identifying the fundamentals of using command line utilities to manage Windows
  - » Using command line tools to manage directories and files
- 

In this chapter, you take a look at several command prompt utilities and a few graphical utilities. Even in the age of Windows, statements that can be issued from a command prompt are still required knowledge for support professionals. This knowledge will help you automate processes — such as batch files — and solve problems when the graphical operating system is not functioning. After reading this chapter, you should have a good understanding of many of the basic commands that are available from the command prompt.

As an added benefit, you find out how to build a basic batch file with some controls in it. This information can be found in Book 6, [Chapter 5](#), and it will surely come in handy on the job.

As an A+ Certified Professional, you will want to use the full range of tools available to you. This chapter introduces you to many of the command line tools that allow you to quickly diagnose and repair problems with operating systems.



**REMEMBER** The A+ exam objectives call for testing on command line tools, which should be limited to the common tools from the exam objectives, which have been listed in this book. To review all possible command line tools for Windows, go to <https://docs.microsoft.com/en-us/windows->

[server/administration/windows-commands/windows-commands](#) or do a web search for *Windows Command line reference A-Z*.

## *Using command.com and cmd.exe*

Many of the really useful utilities in Windows are command line-based. Windows 7 (32-bit) and earlier 32-bit OSes give you two options for running command line utilities: `command.com` and `cmd.exe`.

Windows NT-based OSes, such as Windows 7 through to Windows 10, use `cmd.exe` as the basic command line interpreter for issuing commands. When using `cmd.exe`, you are using a Windows 32-bit application from the point of view of memory management and application stability. `command.com` still exists on these OSes, but it exists for backward compatibility for older applications, and you will only find it on 32-bit systems. As a command line interpreter, there are certain commands which are built into it, and other commands which are read from the Windows directory. This is why you will not find `copy` on your computer, but you will find `xcopy.exe`; `copy` is command which is internal to the interpreter, while `xcopy.exe` is a command which is external to the interpreter, and therefore found in the Windows directory.

Typically, when you want to use a command prompt within Windows, you should run `cmd.exe` by choosing Start ⇒ Run, typing **cmd.exe**, and clicking OK. `cmd.exe` can also be found from the Start menu under All Programs ⇒ Accessories ⇒ Command Prompt in Windows 7 and Windows 8.1, but from the Start menu under Windows System ⇒ Command Prompt in Windows 10. This runs as a 32-bit or 64-bit Windows application (depending on the version of Windows you are running) and thereby can spawn other applications or support standard memory management. Each copy of `cmd.exe` that you execute appears on the process list in Task Manager. If you run `cmd.exe`, the first two lines tell you what executed. Here is an example of what Windows 7 shows:

```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
```

On 32-bit computers, `command.com` on the other hand, is a 16-bit MS-DOS application. It loads a simulated 16-bit environment in the form of `ntvdm.exe` (NT Virtual DOS Machine; NTVDM). You will see `ntvdm.exe` listed on the Process tab of Task Manager. The first two lines listed in this window are

```
Microsoft(R) Windows DOS
(C)Copyright Microsoft Corp 1990-2001.
```

You will notice that, in this case, you are running DOS and Windows 7 (Windows Version 6.1). If you use the command prompt to launch other 16-bit Windows applications, they will be launched within the NTVDM that is executing. The *NTVDM* is the environment that all 16-bit MS-DOS applications and 16-bit Windows applications run in. For more information about supporting these applications, refer to Book 6, [Chapter 2](#).

`cmd.exe` is used when running all other applications. As I mention earlier, it is a 32-bit command prompt with a number of enhancements, including

- » The ability to run 16-bit and 32-bit command line utilities
- » The ability to run POSIX (Portable Operating System Interface for Unix) and OS applications
- » Built-in command history support for saving and executing commands



**REMEMBER** 32-bit versions of Windows use `cmd.exe` as the main command line interface and provide `command.com` for backward compatibility with 16-bit MS-DOS and Windows applications. Remember that `command.com` is not supported on 64-bit Windows operating systems, and the default version of `cmd.exe` is a 64-bit application. Even on a 64-bit version of Windows, Microsoft does provide a 32-bit version of `cmd.exe` for backward compatibility with 32-bit applications.



When you are using any of the command prompt interfaces, you can type `exit` to leave the interface. Remember that the command prompt session may be nested, and `exit` will only leave the current session or level.

## *Executing Your Privileges*

For security reasons, it is not recommended that you log in and run applications using an account that has full administrative rights; rather you should use an account that has normal user rights for all day-to-day operations. There will be times, however, when you need to have elevated permissions to accomplish a task. To aid you in this process Microsoft provided a special command: `runas`.

### *runas*

The `runas` command is used to do just that: run a command as someone else. In most cases you will use it to run a command as a user with administrative rights, but sometimes for testing, you may want to use it to run a command as a user with fewer rights than your normal user.

The basic options required to use the `runas` command are summarized in [Table 5-1](#).

**TABLE 5-1** Switches Used with the `runas` Command

<i>Switch</i>	<i>Description</i>
<code>/noprofile</code>	This switch prevents the profile of the specified user from being loaded. By bypassing the profile, the command can directly execute, but it may fail if information from the profile is required.
<code>/profile</code>	<code>/profile</code> forces the profile or the specified user to be loaded. It is the default option.
<code>/env</code>	Similar to the <code>/noprofile</code> option, the <code>/env</code> option retains the current command environment rather than reloading it as the user.
<code>/netonly</code>	This switch will skip loading the local profile as the credentials are to be used to authenticate to a remote system.
<code>/savecred</code>	This option is used to continue using previously saved credentials.
<code>/smartcard</code>	This option uses credentials from a smartcard.

<b>Switch</b>	<b>Description</b>
<code>/user</code>	The <code>/user</code> option specifies the user credentials to use for running the specified command in the form <code>user@domain</code> or <code>domain\user</code> .
<code>/showtrustlevels</code>	This switch displays the trust levels that can be used for the command.
<code>/trustlevel</code>	This switch specifies a trust level to use for the command.
<code>program</code>	The name of the program and any command line option that are to be used. If any spaces occur, the entire command is required to be in quotes. If quotes are needed by the command inside of quotes, inner quotes should be preceded by the escape character <code>\</code> .

To run the command `regedit.exe` as the local Administrator account, the command would be similar to the following:

```
runas /profile /user:Contoso\Administrator "reg.exe import \"C:\MyRegFile.reg\""
```

If you prefer to not use the command line, you can also access this functionality for applications by selecting the application, pressing the Shift key, right-clicking, and then selecting Run as Different User. This action will present you with a logon dialog box that will be tied to the application.

## *Using commands with privilege*

Even when you are logged into an account that has administrator privilege, you still may not be able to run certain commands. For example, if you are going to use a command that has potential to do damage or make the computer inoperable, then you will likely need to have privilege. To get the elevated privileges you need, run the Administrator Command Prompt. The Administrator Command Prompt is there to prevent accidental execution of dangerous commands. Think of it as User Access Control (UAC) for the command prompt.

To run the Administrator Command Prompt, locate a shortcut to the command prompt by selecting Start, type **cmd**, right-click the shortcut, and select Run as Administrator. With Windows 7 and newer OSes, you can right-click on a running command prompt in the Taskbar, right-click command prompt in the menu, and then select Run as Administrator.

The following commands require that you have administrative privilege and be using the Administrative Command Prompt in order to properly run them:

» `chkdsk.exe`

» `defrag.exe`

» `diskpart` (does not require administrative command prompt, but does require a UAC prompt if not using an administrative prompt)

» `shutdown`

Each of these commands is covered in detail later in this chapter. Remember, when you run a command and do not get the expected output, it may be that you do not have the rights to see what is missing.

## *Managing Directories*

All files that are saved to disk are stored in a hierarchical directory structure. All the files could be placed at the top of this structure, but it would be disorganized, and therefore poorly managed. Also, most top-level directories, or *root directories*, can hold a limited number of files. This directory structure can hold as many nested sub-directories as you want. The commands discussed in the following sections allow you to get listings of files as well as create and delete directories on your disk.



**REMEMBER** All command line tools in this section have not changed substantially since MS-DOS, but some have a few more options than they used to have.

### *dir*

The first command that you will see is the directory command (`dir`). This command is used to get a listing of the files that are in a directory on your disk. Using `dir` by itself gives you the listing of your current directory. The current directory is usually listed in the command prompt, like this:

```
C:\WINDOWS>_
```

The `dir` command is very useful and has several options, discussed later in this section. First, though, you need a firm grasp of wildcards, relative paths, and absolute paths.

## *Wildcards*

Two wildcards can be used to modify what results you receive: `*` and `?`. These can be used multiple times in different combinations in the same command to filter the results.

The `*` wildcard represents one or more characters. Here is an example of using the `*` wildcard to retrieve a list of files that match a certain pattern. The command

```
dir WIN*.*XE
```

returns the following:

```
WindowsAnytimeUpgradeResults.exe
wininit.exe
winload.exe
winlogon.exe
winresume.exe
winrs.exe
winrshost.exe
WinSAT.exe
winver.exe
```

The results include all files that start with `win` and end with `xe`, with any number of characters in between — even zero. These wildcards are also useful when used in conjunction with `copy` commands, which I discuss later in the chapter.

The `?` wildcard character works a little different than `*` because `?` represents one or zero characters. Here is an example of `?` in action, as it looks for all files that were created on the fifth of any month after Jan 01, 2000, given that all the filenames match their dates using eight-character numeric dates with the pattern of `mmddyyyy.txt`. The command

```
dir ??052???.TXT
```

would return the following list of files:

```
01052000.TXT
05052000.TXT
10052000.TXT
11052000.TXT
12052000.TXT
04052002.TXT
12052003.TXT
06052008.TXT
```

The `?` in the command doesn't return any files that have more than two characters before the `05` and doesn't return any more than three characters after the `2` in the `dir` statement.

### *Relative paths and absolute paths*

When you use `dir`, you are given a directory listing for your current directory. To see the listing for a different directory, [Table 5-2](#) provides several options for choosing a different directory. All the command examples in the table use this directory structure:

```
c:\parent_dir\child_dir\grandchild_dir
```

**TABLE 5-2** Ways to Specify Directory Paths

<b>Command</b>	<b>Directory Result</b>
<code>dir</code>	Returns the listing for the current directory <code>c:\parent_dir\child_dir.</code>
<code>dir c:</code>	Returns the listing for the current directory on the C: drive <code>c:\parent_dir\child_dir.</code>
<code>dir c:\parent_dir</code>	Returns the listing for <code>c:\parent_dir.</code>
<code>dir \</code>	Returns the listing for the root of the current drive <code>c:\.</code>
<code>dir ..</code>	Returns the listing for the parent directory of the current directory <code>c:\parent_dir.</code>
<code>dir ..\..\</code>	Returns the listing of the parent directory of the parent directory of the current directory <code>c:\.</code>

<b>Command</b>	<b>Directory Result</b>
dir ..\child_dir	Returns the listing of a directory named <code>child_dir</code> , which is a child of the parent directory c:\parent_dir\child_dir.
dir grandchild_dir	Returns the listing of a child directory named grandchild_dir: \parent_dir\child_dir\grandchild_dir.

with the current directory set to `c:\parent_dir\child_dir`.

Whenever a full path is specified, starting with the drive letter, it is referred to as an *absolute path*. If you do not specify the full path, you are using a *relative path*. Care should always be taken when using relative paths with commands. Look, for example, at the following code sample:

```
dir sub_dir
del *.*
```

In this example, a directory (`dir`) listing is taken of a sub-directory (`sub_dir`), and the following delete (`del`) command was working on the entire contents of the current directory, not the directory listing which was just retrieved. This is an easy mistake to make. When working with relative paths, double period (`..`) notation refers to a parent directory, and single period (`.`) notation refers to the current directory.

Most programs and commands can have their actions modified by providing options on the command line. These options are usually represented by one or more letters and are introduced to the command with either `/` or `-`. The `-` character is usually used with commands that come from (converted from) the Unix OS, but most MS-DOS programs have implemented `/`. These options are referred to as *switches*. `dir /on /s` is an example of the `dir` command using switches.

[Table 5-3](#) summarizes some of the most important switches for the `dir` command.

### **TABLE 5-3** Switches for `dir`

<b>Switch</b>	<b>Description</b>
---------------	--------------------

---

Switch	Description
--------	-------------

---

/ax	The /a switch is short for <i>attributes</i> . This switch provides a listing of files that have matching attributes. This switch must be used in conjunction with an additional letter to provide results. Five letters may be used: (d)irectory, (a)rchive, (h)idden, (s)ystem, and (r)ead-only. Using a minus sign with one of these five letters reverses the listing: For example, /a-d shows you things that are not directories.
-----	---

---

The /b command displays a bare listing. A *bare listing* does not include a separate section in the output that tells you the directory that you are working with, but rather displays a single-line listing, like this output from these example commands:

/b	<pre>dir /b /s c:\windows\system32\bcd*.exe c:\windows\system32\bcdboot.exe c:\windows\system32\bcdedit.exe dir /b c:\windows\system32\bcd*.exe bcdboot.exe bcdedit.exe</pre>
----	---

---

/ox	The /o switch is short for <i>order by</i> . This switch is similar to /a in that /o also requires an additional letter to tell it how to order or sort. The options available for sorting are (n)ame, (s)ize, (e)xtension, (a)ccessed date (earliest first), and (d)ate modified (earliest first). Using a minus sign (for example, /o-d) reverses the order. If you use the letter g after the o (for example, /ogd), directories will be grouped at the top of the list rather than mixed in.
-----	--

---

/s	This switch includes listings for each sub-directory under the directory listing.
----	---

---

---



**TIP**

In this chapter, you see many switches for each of the command line tools, but these are not all the possible switches. To see the complete list, type the command with a /? after it, like this:

```
dir /?
```

If you want to use the same set of switches each time you execute the `dir` command, use the `dircmd` environment variable. This variable can be set in the `autoexec.bat` file or at a command prompt, like this:

```
set dircmd=/on /w
```

Now, every time you use `dir`, you will get output that looks like this:

```
Volume in drive C is DRIVE_C
Volume Serial Number is FC26-B8E0
Directory of C:\Windows\panther

[.] [..] cbs.log
Contents0.dir Contents1.dir DDACLSys.log
diagerr.xml diagwrn.xml [FastCleanup]
MainQueueOnline0.que MainQueueOnline1.que setup.etl
[setup.exe] setupact.log setuperr.log
setupinfo [UnattendGC]
12 File(s) 1,002,964 bytes
5 Dir(s) 24,540,774,400 bytes free
```



**TIP**

Note that the list is presented in wide format and sorted by name.

If you are using Windows and you want the setting of the `dircmd` variable to be saved, add the variable by using the Environment Variables settings in the System Control Panel, which you can get to by choosing Properties when you right-click Computer (or This PC for Windows 8.1 or newer users) to open the System Properties dialog box; then click the Advanced System Settings link and the Environment Variables button.

## *md*

`md`, or `mkdir`, is used to create directories; there is no difference between the two commands other than their spelling.

## WHY DOES ONE COMMAND HAVE DIFFERENT NAMES?

Many commands used with MS-DOS originated in other operating systems, such as UNIX and Linux; in some cases, new short forms were created to make them easier to use. To provide backward compatibility, support for the older spelling of the command was also kept.

The directory created will be in the current directory unless you provide an alternative path to the command, like this:



```
md "c:\temp\my new directory"
```

## *cd*

`cd`, or `chdir`, is used to change the current directory for a drive to another directory. The drive need not be your current drive; this command can set a current directory on another drive. For example, if your current drive is `C:`, you could still use `cd d:\my_dir_on_d` to change the current directory for the `D:` drive. You will not see a difference onscreen, but if you change to the `D:` drive by using `d:`, you will see that the current directory is set to `d:\my_dir_on_d`. The current directory is important when you want to use other file operation commands, such as `copy`. If you only specify the drive that you want to work with, you will be working with the current directory on that drive. Take a look at this example:

```
D:\somedirectory\>c:
C:\Documents and Settings\ed\>cd \
C:\>mkdir d:\old_configs
C:\>cd d:\old_configs
C:\>copy a*.bat d:
C:\>copy c:\c*.sys d:\old_configs
```

The first line changes your current drive to `C:`. The second changes to the root directory of the current drive (`C:\`). The third creates a new directory on the `D:` drive, and the fourth line sets `old_configs` as the current directory on the `D:` drive. You will see the `copy` command in the upcoming section “[copy](#),” but the fifth line copies all files in the current directory that start with `a` and end with `.bat` to the current directory on the `D:` drive (currently `old_configs`). The last line copies all files from `C:\` that start with `c` and end with `.sys` to `d:\old_configs`. Lines 5 and 6 copy files from the same directory (`C:\`); the relative path is used in line 5, and the absolute path is used in line 6. The destination directory in line 6 is also absolute, and the relative path or current directory is used in line 5. In both statements (lines 5 and 6), the same directories are used as the source and destination directories.



**WARNING** Relative paths can save on typing, but they can also cause errors if you are not careful.

## *rd*

`rd`, or `rmdir`, is used to remove or delete directories from your drive. Two rules are imposed on you: Before you delete a directory

- » The directory must be empty.
- » It cannot be the current directory.

You can *empty* a directory by using the `del` command to delete the files or use the `/s` option to delete sub-directories and any files they contain. To remove a directory, though, just specify its location after the `rd` command:

```
rd c:\remove_me
```

# *Copying and Moving Files*

Doesn't it seem like when you finally get things organized, it's time to start all over again? When organizing and backing up files, you will often be required to copy or move files to new locations, either in another directory or on another disk. The following sections provide an overview of the commands that help you with these tasks.

## *copy*

The `copy` command expects you to give at least the name of the file you would like to copy. If you provide only one filename, the selected file is copied into the current directory. If you provide a source filename and a destination directory by using a command like

```
copy c:\source\myfile.txt c:\destination
```

the file will be copied into the destination directory. You can also rename files while you are copying them by using a command like this:

```
copy c:\source\*.bat c:\destination\*.old
```

The preceding command would copy all files with an extension of `.bat` from the source directory and rename them with an `.old` extension in the destination directory.

If you are about to overwrite an existing file, you will be prompted to confirm the operation. This can be suppressed if you use `/Y` at the end of your `copy` command. `/Y` answers “yes” to the `copy` command's “confirm overwrite?” question. If you want to consistently overwrite destination files, you can set the `copycmd` environment variable to `/Y` in the same manner that you set the `dircmd` variable in the “[dir](#)” section, earlier in this chapter.

## *xcopy*

Many times, you have to copy entire directory structures from one location to another. If you were to do this with the `copy` command, you would first have to create all the destination directories by using the `md` command. When using the `xcopy` command, though, you can perform this task in a minimal amount of time. To copy an existing directory named `source` to a new directory named `destination`, you would issue the following command:

```
xcopy c:\source\*. * c:\destination\*. *
```

To copy all the sub-directories as well, use

```
xcopy c:\source\*. * c:\destination\*. * /s
```

To also include empty directories, add the `/e` (empty) switch to the end of the command. To include just files with the archive attribute set, add the `/a` (archive) switch.

Like the `copy` command, adding `/Y` will overwrite files without asking for confirmation. The `/Y` tells the command to answer “yes” to all overwrite prompts.

## *robocopy.exe*

The `robocopy.exe` command is a turbocharged version of the `xcopy` command used to copy files and directories between locations. As with `xcopy`, you need to specify at least a source directory and a destination

directory. To copy an existing directory named `source` to a new directory named `destination`, you would issue the following command

```
robocopy.exe c:\source c:\destination
```

The `robocopy.exe` command supports a wide variety of options — and some of the most common are listed in [Table 5-4](#) — but if you are interested in this useful command, explore all the options using `robocopy.exe /?`.

**TABLE 5-4** Switches for `robocopy.exe`

Switch	Description
<code>/e</code>	The <code>/e</code> switch copies all source directories to the destination location, including empty directories.
<code>/purge</code>	The <code>/purge</code> option deletes destination directories that no longer exist in the source directory. This may be the case if you are running the <code>robocopy.exe</code> command a second time, after making changes to the source directory.
<code>/z</code>	The <code>/z</code> command copies the files in restartable mode, which is useful if copying large files over a slow network. If the file copy is interrupted, it can pick up in the middle of the file it was working on, rather than starting at the beginning of the file.
<code>/b</code>	This switch copies the files in backup mode, which may be necessary if you have files that open by users, and <code>robocopy.exe</code> cannot get a lock on the file. Backup mode allows for files to be copied without putting locks on the files.
<code>/copyall</code>	This switch copies all file properties, including data, attributes, time stamps, NTFS permissions, owner information, and auditing information.
<code>/mir</code>	The <code>/mir</code> switch is the same as running <code>robocopy.exe</code> with both the <code>/e</code> and <code>/purge</code> switches.
<code>/mot:m</code>	This option monitors the source directory, and will rerun the <code>robocopy.exe</code> command again if any changes are found within the number of minutes defined by the <code>m</code> .
<code>/r:n</code>	The option should be a mandatory option; it specifies how many times <code>robocopy.exe</code> should attempt to copy failed files. Specify the number of attempts with the <code>n</code> . The default is one million attempts.
<code>/w:n</code>	The <code>/w</code> switch works with <code>/r</code> , as it is the time in seconds ( <code>n</code> ) to wait between attempts to copy the failed files. The default is 30 seconds.
<code>/v</code>	To see a list of all the files that are copied, use the <code>/v</code> switch.

<b>Switch</b>	<b>Description</b>
<code>/log:file</code>	This switch creates a log file, listing all the files that are copied, and saves it in the file specification that follows the colon.

When `robocopy.exe` has completed its operation, it will display a summary. Here is an example of `robocopy.exe` copying a small `temp` directory with a sub-directory to a new location, `temp2`.

```
C:\>robocopy.exe /mir /v c:\temp c:\temp2

-----
ROBOCOPY :: Robust File Copy for Windows
-----

Started : Fri Apr 06 20:57:25 2012
Source  : c:\temp\
Dest    : c:\temp2\
Files   : *.*
Options : *.* /V /S /E /COPY:DAT /PURGE /MIR /R:1000000 /W:30

-----

New Dir 1 c:\temp\
100% New File 24 autoexec.old
New Dir 1 c:\temp\sub\
100% New File 24 autoexec.bat

-----

Total Copied Skipped Mismatch FAILED Extras
Dirs : 2 2 0 0 0 0
Files : 2 2 0 0 0 0
Bytes : 48 48 0 0 0 0
Times : 0:00:00 0:00:00 0:00:00 0:00:00
Ended : Fri Apr 06 20:57:25 2012
```

From the output, you should see that two directories were created and two files were copied. Two of the biggest advantages of `robocopy.exe` are the ability to refresh a previously copied directory by only updating changed files and to resume failed copy operations.

## *move*

The `move` command moves files from one directory to another. It is also used to rename directories. To use the `move` command, you have to

specify the name of the files you want to move and then specify the destination directory, like this:

```
move c:\source\source_file.txt c:\destination\
```

To rename the directory `c:\source`, you can use

```
move c:\source destination
```

## *del*

To delete or remove files or directories, you can use `del` or `erase`. Like earlier examples, these two commands are synonymous. If you want to delete multiple files, you have to use the `*` and `?` wildcards. (Read about wildcards earlier in this chapter.) Windows allows you to delete directories with this command, and you can use `/s` to delete files from all sub-directories as well. If you do not want to be prompted to confirm deletions, use `/Q` for quiet. To select files to delete based on their attributes, use `/A` in the same manner as the `dir` command.



**WARNING** It is very easy to unintentionally delete files (or delete the wrong files) when working with relative paths. When possible, use full pathnames to avoid mistakes.

## *ren*

The `ren` command is used to rename files and directories. Similar to many of the commands that you have looked at, you specify the source name and a new name for the file or directory.

# *Performing Diagnostics and Tuning Performance*

At the command prompt, a few commands can be used to optimize and diagnose your computer. `defrag.exe` can be used to optimize your hard drive, and `chkdsk.exe` can be used to check your disk for errors.

The command prompt versions of the `defrag.exe` and `chkdsk.exe` utilities have now been replaced by Windows versions, but these commands are great if you are creating scripts or batch files to perform these actions.

## *defrag.exe*

The purpose of the `defrag.exe` utility is to fix speed and performance problems with hard drives. As files are written to and then deleted from a disk, they leave holes or blank areas scattered around your drive. When you write files to a disk, they always write to the largest open spaces that are available to them. There will be times when the largest area is not large enough for the entire file, and the file will have to be split into pieces. These *fragmented* files are slower to access because the disk head has to keep moving to a new location on the drive. To defragment the files on your hard drive, use Computer Management in Windows, or `defrag` from the command line. To assist users with scripting solutions to use most tools, or to allow them to run the commands through command line only sessions on a server, Microsoft provides command line access to most Windows-based utilities.



TECHNICAL  
STUFF

With the popularity of solid state drives (SSD), you do not need to worry as much about defrag. Defragmenting a drive eliminates a drive head seek delay, but SSDs do not have heads that need to move. Since the OS has a limit to the fragmentation it can function with, Windows 10 will periodically defragment your drive.



TIP

For more information about using Computer Management in Windows, see Book 6, [Chapter 4](#).

## *chkdsk.exe*

`chkdsk.exe` serves an important purpose within the Windows operating system. Its job is to check

- » The directory structure and directory entries for corruption
- » The disk for worn-out areas

Its purpose is to reduce the chance of data loss by catching corruption early and by fixing small problems before they become larger.



**TIP**

For more information about `chkdsk.exe`, read Book 6, [Chapter 4](#).

## ***shutdown.exe***

`shutdown.exe` is listed here as a diagnostic tool as it allows for the shutdown of the local computer or of a remote computer. This is useful when you want to perform a reboot at the end of a batch file or need to remotely reboot a computer which you have been performing maintenance or troubleshooting on. [Table 5-5](#) summarizes the main options for the `shutdown.exe` command.

**TABLE 5-5 Switches for shutdown.exe**

<i>Switch</i>	<i>Description</i>
<code>/?</code>	This option displays help information for the command.
<code>/i</code>	This option displays the GUI window to let you execute the command with various options, but in a graphical manner.
<code>/l</code>	This option logs the current user off, but does not shut down the computer.
<code>/s</code>	<code>/s</code> shuts down the computer.
<code>/r</code>	<code>/r</code> shuts down and restarts the computer.
<code>/g</code>	<code>/g</code> shuts down and restarts the computer, and then restarts any registered applications.
<code>/a</code>	This switch aborts a previously scheduled shutdown command.



<b>Switch</b>	<b>Description</b>
<code>/h</code>	The <code>/h</code> switch tells the computer to hibernate rather than shut down.
<code>/e</code>	This option records the reason for the unexpected shutdown.
<code>/m</code> <code>\\computername</code>	This option issues the command against a remote computer rather than the local computer. If you forget this option, you will be shutting down the local computer, which is an inconvenient and common mistake.
<code>/t xxx</code>	With this switch, time before the shutdown command is executed. The default is 30 seconds, but can be number of seconds up to 10 years in duration.
<code>/c "Comment"</code>	This option comments on the reason for the shutdown. You are limited to 512 characters.
<code>/f</code>	<code>/f</code> forces running applications to be closed. Unsaved data in applications will be lost.
<code>/d [p u]xx:yy</code>	This option provides the reason you are using the shutdown command to the shutdown tracker. The shutdown is either Planned or Unplanned. Refer to the output of the help command to determine appropriate values to use in the xx and yy positions.

A typical shutdown command to reboot a remote computer named `testpc` would look like:

```
shutdown.exe /t:60 /r /m \\testpc
```

## *tasklist*

The `tasklist` command is used to display the currently running tasks or presses. This is the same list you can see if you run the Task Manager, which is covered in Book 6, [Chapter 3](#).

Tasklist run by itself shows you all the processes running on the computer and displays the following information:

- » **Image name:** The name of the executable that is running.
- » **PID:** The process ID is a unique number assigned to the process.
- » **Session name:** The session that is running the process. There will be a services and console session in addition to sessions for each user actively on the computer.

- » **Session#:** Each session will have a corresponding number, with services being 0 and the console being 1.
- » **Mem Usage:** The amount of memory (physical and virtual) being consumed by the process.

To see verbose output, you can use the switch `/V`, which adds Status, User Name, CPU Time, and Window Title to the information displayed. To change the format of the output, you can use the switch `/FO`, which takes the parameters Table, List, or CSV, the latter used to export the data to Microsoft Excel or a spreadsheet application. Finally, you may also use the switch `/FI` to filter the data being displayed by any of the display columns. Use the `/?` Switch to view all the options for filtering. You are able to use the `/FI` option multiple times to filter the list down to exactly what you are looking for.

## *taskkill*

To go along with `tasklist` there is the `taskkill` command. In the same way that you will go to Task Manager to terminate applications or background processes, you may want to use `taskkill` to terminate these processes. To terminate a process with the `taskkill` command, you will need to specify a PID (`/PID`), an image name (`/IM`), or a filter (`/FI`), which specifies multiple processes to remove. The filter options for `taskkill` are the same as for `tasklist`, so you can use `tasklist` to ensure that you are correctly filtering the list of processes to kill. Here is a sample `taskkill` command to terminate all copies of `notepad.exe` running on a computer named Win7-AP1:

```
taskkill /S Win10-AP1 /U Win10-AP1\Administrator /FI imagename eq notepad.exe
```



TECHNICAL  
STUFF

Using the switch `/S` enables you to run both the `tasklist` and the `taskkill` commands against another computer on the network, rather than against your local computer.

# Getting Active with Group Policy

Microsoft Active Directory (AD) stores and applies configuration settings to both users and computers that are members of the AD domain. These settings are stored in Group Policy Objects (GPO) and are automatically applied every 90 minutes as well as when the computer starts up and when a user logs on. Two commands are helpful when working with GPO settings: `gpupdate` and `gpresult`.

## *gpupdate*

It is not always possible to wait 90 minutes to have a GPO change show up on your computer. If you were to always have to wait, then testing of changes would take days or weeks. The solution to this waiting is `gpupdate`, which can be used to force an immediate update of the client-side policy settings. The settings in the GPO can be targeted to the user or to the computer. [Table 5-6](#) lists the options that are used with `gpupdate`.

**TABLE 5-6** Switches for `gpupdate`

Switch	Description
<code>/Target: {Computer User}</code>	By default, both user and computer policies are updated when the <code>gpupdate</code> command is executed. <code>/Target</code> allows you to specify just user or computer policies.
<code>/Force</code>	This option applies all policies again, rather than only the changed policies.
<code>/Wait:{Value}</code>	This option specifies the amount of time for policy processing to complete. The default time is 600 seconds.
<code>/Logoff</code>	This option logs the user off after the policy processing is completed. Some policy processing of user settings requires that the user logs off in order for the settings to take effect. Folder redirection would be one example of these settings. This setting is ignored if there are no relevant settings applied.
<code>/Boot</code>	This option triggers a reboot after the policy processing is complete. Some policy processing of computer settings requires that the computer restarts in order to apply the settings. An example of this setting would be computer-targeted software installations. This switch will be ignored if no relevant settings are processed in the policy.

The following example command performs an update of user settings and processes all policy settings:

```
gpupdate /target:user /force
```

## *gpresult*

When you want to know what policies are being applied to a computer or to a user, `gpresult` is your friend. The `gpresult` command generates a report or listing of all the settings that have been applied through the series of GPO updates that relate to the user or computer. This report is also referred to as Resultant Set of Policy (RSoP). [Table 5-7](#) show the most common switches used by `gpresult`.

**TABLE 5-7** Switches for `gpresult`

<i>Switch</i>	<i>Description</i>
/S system	Rather than running against the location machine, /S allows you to specify a remote computer for the command.
/U domain\user	Using this option allows you to run the command as another user.
/P password	Use this option to provide the password for the specified user.
/SCOPE scope	This option specifies if the results should be generated for the “USER” or the “COMPUTER.”
/USER domain\user	This option specifies which user for which you would like to evaluate the policies.
/X filename	Use this option to generate output files in an XML format.
/H filename	Use this option to generate output files in an HTML format.
/F	This option will overwrite existing output files.
/R	To display the Resultant Set of Policies (RSoP), you will use this option.
/V	This option will provide verbose output.
/Z	If verbose is not enough, this option will provide super verbose output.

The following is an example of the `gpresult` command in action. This command will generate an HTML report for computer-based GPO settings and will include verbose information:

```
gpresult /H c:\GPResult.html /SCOPE COMPUTER /V
```

After it is generated, the report can be viewed in Internet Explorer.

## *Working with Other Useful Commands*

The rest of the utilities in this chapter defy easy classification. Although they serve a wide range of functions, they are all important in your computer's usage.

### *attrib.exe*

All files have five basic attributes:

- » a: Archive. Files that have been modified.
- » h: Hidden. Are not usually visible.
- » i: Not to Be Indexed. Should not be included by the system indexing service. This attribute was added in Windows Vista.
- » r: Read-only. Cannot normally be deleted, nor can they be modified.
- » s: System. Have special file protection so that you may not delete or modify them.



**TIP**

The archive attribute is used by some backup utilities to identify changed files for incremental backups.

The `attrib` command allows you to change these attributes. The attributes are added or removed from files by specifying the attribute with a `+` or `-` character in front of the filename, as in the following statement:

```
attrib -s -h +a +r c:\*.sys
```

The preceding statement removes the system (`s`) and hidden (`h`) attributes while adding the archive (`a`) and read-only (`r`) attributes. Adding `/s` to

the end of the line would apply the same attributes to all the files in the sub-directories as well.

## *diskpart.exe*

To manage disk partitioning, if the need ever arises, Windows uses the Disk Management graphical disk partitioning tool. Windows also uses another command line tool: `diskpart.exe`. Although this tool is capable of all disk partitioning tasks, you need to use this tool only to perform rare disk partition changes that Disk Management cannot perform, such as expanding a partition on a basic disk. The need to use `diskpart.exe` has been reduced with the introduction of Windows 7, which incorporates the ability to expand those partitions into the Disk Management graphical tool.

The reason for not using `diskpart.exe` is that its user interface is awkward. To illustrate the interface, [Listing 5-1](#) holds the steps required to create a partition on a disk and format the drive (extra blank lines have been removed):

### **LISTING 5-1 Creating a Partition on a Disk and Formatting the Drive**

---

```
C:\>diskpart.exe
DISKPART>list disk
Disk ### Status Size Free Dyn Gpt
-----
Disk 0 Online 6142 MB 0 B
Disk 1 Online 510 MB 0 B
Disk 2 Online 6142 MB 6142 MB
DISKPART> select disk 2
Disk 2 is now the selected disk.
DISKPART> create partition primary size=1000
DiskPart succeeded in creating the specified partition.
DISKPART> list partition
Partition ### Type Size Offset
-----
Partition 1 Primary 1004 MB 32 KB
DISKPART> select partition 1
Partition 1 is now the selected partition.
```

```
DISKPART> assign letter=f
DiskPart successfully assigned the drive letter or mount point.
DISKPART> exit
Leaving DiskPart...
C:\>format f: /fs:ntfs
The type of the file system is RAW.
The new file system is NTFS.
WARNING, ALL DATA ON NON-REMOVABLE DISK
DRIVE F: WILL BE LOST!
Proceed with Format (Y/N)? y
Verifying 1004M
Volume label (ENTER for none)? More Data
Creating file system structures.
Format complete.
1028128 KB total disk space.
1020600 KB are available.
```

This process could have been completed through a single wizard in Disk Management, with less effort.

## ***format.com***

Using the `format.com` command prepares a disk to be used by your computer. The purposes of this command are to

- » Check whether all clusters on the partition are in working order.
- » Create the directory table.

On FAT partitions, the directory table is referred to as the *File Allocation Table*. The directory table maintains a list of where each file starts on the disk.

The `format` command requires a drive letter and supports additional switches. The proper syntax to format your A: drive is

```
format a:
```

You could modify the command by adding `/q` to the end of the line to perform a quick format of the drive.



**TIP**

The quick format doesn't check the integrity of the sectors on the drive but only deletes and re-creates the directory table.

You can use `/FS:filesystem` to specify the format of the partition as FAT, FAT32, exFAT, UDF, or NTFS, and Windows 8.1 adds support for RdFS.

## *dism.exe*

The Deployment Image Servicing and Management (`dism.exe`) tool is used to service, or change, Windows images. This image could be in the form of an image file (`.wim`, `.vhd`, or `.ffu`) or an installed copy of Windows. This tool has been available since Windows 7 and is now part of the operating system, but it can also be found as part of the Windows Assessment and Deployment Kit (ADK).

The command syntax is too extensive to be covered here, but the key root level commands are listed in [Table 5-8](#).

**TABLE 5-8 Switches for `dism.exe`**

<b>Switch</b>	<b>Description</b>
<code>/Get-ImageInfo</code>	Displays information about the image file specified.
<code>/Commit-Image</code>	Saves changes made to the files in a mounted image.
<code>/Mount-Image</code>	Mounts the contents of an image file to a directory on your drive.
<code>/Unmount-Image</code>	Disconnects a mounted image from a directory on your drive.
<code>/Capture-Image</code>	Copies a drive or drive partition into an image file.
<code>/Apply-Image</code>	Copies files from an image file to a drive or drive partition.
<code>/Online</code>	Runs the command on the current running operating system rather than an image file.



To find out more about each command, type `/?` after an option like this:

```
dism.exe /Online /?
```

## *sfc.exe*

`sfc.exe` is the System File Checker and is used to verify the integrity of protected operating system files. This tool is not only capable of scanning and verifying files, but it is also able to repair files that are no longer valid. More information about this command can be found in Book 6, [Chapter 4](#).

## *net.exe*

The `net.exe` command has been around since MS-DOS first added networking services. This tool had been enhanced over the years, but the basic functionality has remained constant. This tool is used to manage network users and connections. Two main options appear on the A+ exam objectives: `Use` and `User`.

The command `net.exe /User` is used to manage users on your computer or domain. You are able to create users, delete users, set a new user password, set logon times, and disable or enable users. The basic command to create a user named Bob would look like this:

```
net User Bob P@ssword /add
```

To add this user to a local group or domain group, you are able to `net.exe /LocalGroup` or `net.exe /Group`.

After creating a user, that user can log on and connect to network resources. If you want to connect to a network share you can use `net.exe View \\ComputerName` to see a list of shared folders on the computer, `ComputerName`. Once you know the name of a share you want to connect to, you can connect a shared folder to drive `M:` using a command like this:

```
net.exe M: \\ComputerName\Share /User:Bob /Persistent:Yes
```

This command will connect to the resource as the user `Bob` and `Persistent` will reconnect the drive during the next reboot.

## *help*

If you need to know how to do something with the command line, you have two main options. All commands support `/?` as a switch to get additional information on how to use the command. Additionally, Windows also has a `help` command.

Use `help` followed by the command that you would like to get help on: for example

```
help help
```

If you use `help` by itself, you get a list of commands that you can request help for.

## *Getting an A+*

The most important things to remember from this chapter are what the different commands are used for and the major differences between similar commands. Here is a quick review:

- » `attrib` changes file attributes, such as read-only, hidden, system, and archive.
- » `copy` copies one or multiple files from one directory to another.
- » `defrag` defragments your hard drive to increase performance.
- » `dir` displays a list of files in a directory or directories.
- » `format` prepares a disk for accepting data or to erase a disk.
- » `chkdsk` checks a disk for errors that could cause data loss.
- » `net.exe` is used to manage network items, which includes users and drive mappings.
- » `xcopy` is like `copy` but can be used to copy entire directory structures.

## *Prep Test*

- 1. You are working on the help desk, and you receive a call from Mary. She is looking for a file that is saved on her hard drive. She has forgotten the name she gave it, but she knows that the title**

**contains the word “budget” and that it is a Microsoft Excel spreadsheet. What command will best help her locate her document?**

- (A) `dir *budget.xls`
- (B) `dir *budget*.xls /b`
- (C) `dir *.budget*.xls /s`
- (D) `dir *budget*.xls /b /s`

**2. You need to regularly back up files in a directory, but you want to back up only files that have changed. What commands can you use to accomplish this in the easiest way possible?**

- (A) `fc` and `xcopy`
- (B) `attrib` and `copy`
- (C) `fc`, `changes`, and `xcopy`
- (D) `xcopy` and `attrib`

**3. You want to copy a directory structure (complete with sub-directories), so you use `copy c:\dir1\*. * c:\newdir /s /e`. What will you find in the `newdir` directory?**

- (A) All files that were in `dir1`
- (B) All files and sub-directories that were in `dir1`
- (C) Nothing — the command is improperly constructed and will generate an error
- (D) None of the above

**4. You receive a call from a user on your network complaining that his computer is slow. You ask a few more questions and find out that he feels that the speed of his hard drive is much slower than when he got his computer. What command would you suggest running?**

- (A) `diskfix`
- (B) `bootrec`
- (C) `scanfix`

(D) defrag

**5. You are working on a co-worker's computer and you notice that you are missing a drive connection to drive P: for \\Server\Public. You need to access files on the P: drive. What command would you suggest running?**

(A) `Net User P: \\Server\Public /Persistent:Yes`

(B) `Net Use P: \\Server\Public /Persistent:Yes`

(C) `Net User P: \\Server\Public /Persistent:Yes /Domain`

(D) `Net Use P: \\Server\Public /Persistent:Yes /Domain`

## Answers

1. **D.** Although C looks like a good choice as well, using the sub-directory switch, it has an additional period in the search string, so will not return as many files and will work only if Mary's document has a period in front of the word *budget*. See "[dir.](#)"
2. **D.** The `attrib.exe` command can be used to remove the archive attribute from all files in a directory structure. Then, as files are modified, you can use `xcopy *.* c:\backuplocation /s /a` to copy all the files to a new location. If you want your next copy to copy the files that were modified since the last copy, you have to use the `attrib` command to remove the archive attribute again. Check out "[xcopy.](#)"
3. **C.** The suggested command will cause a syntax error, and nothing will be copied. The `copy` command does not support either `/s` or `/e`; to use these options, you have to use the `xcopy.exe` command. Peruse "[xcopy.](#)"
4. **D.** `defrag` is used to reorganize files, which speeds up access to the disk. Check out "[defrag.exe.](#)"
5. **B.** The correct command would be `Net Use P: \\Server\Public /Persistent:Yes`. Two of the wrong answers use `Net User`, which

is used for user management and not drive mappings. The incorrect `Net Use` command has the `/Domain` switch, which is used on the `Net User` command when managing a user in a domain. *Look back at [“net.exe.”](#)*

# Chapter 6

## Working with System Files and the Boot Process

---

### IN THIS CHAPTER

- » Identifying the names and purposes of each file required to boot up a Windows 7 or newer computer
  - » Identifying the locations of Windows 7 or newer boot files
- 

Starting a computer has long been referred to as *booting*. Before you can use your computer, you need to be able to boot it to a point where the operating system (OS) is functional. Otherwise, your computer is like a safe without a known combination. This chapter will help you get that “safe” open by examining the boot process, which encompasses a series of steps, from powering-on to loading the OS shell. This chapter reviews the hardware *POST* (*power-on self-test*) process and will concentrate on the OS portion of the overall process. This chapter also introduces you to the standard Windows boot process and the files that are required, and also how to correct or deal with boot problems related to the boot files. A solid understanding of the Windows boot files will prepare you for the A+ exams, and a general knowledge of the other files will prepare you for working with these systems in the field.

If, as an A+ Certified Professional, you are faced with troubleshooting the boot process on a computer for a user, it is required that you understand the boot sequence. If you do not know what the normal boot process is, you will be at a deficit attempting to troubleshoot issues with it. As a CompTIA A+ Certified Professional, you will often have to bring your knowledge of the core operating system files to bear on your user’s computer conundrums.



FOR THE  
EXAM

If you are unfamiliar with boot processes in general, focus on the entire chapter. The A+ exams, though, focus on the Windows boot process.

## *The Power-On Self-Test (POST) Process*

The *power-on self-test (POST)* process starts when power is applied to the system. Electrical current makes its way from the power lead on the motherboard to the ROM-BIOS chips; when the current is received by the BIOS chips, they immediately begin executing their programs. One of the first checks is the memory (both a count and integrity test). After the memory check, the POST process moves on to find out what ports or I/O devices exist on the system. If the system is equipped with a PnP (Plug and Play), as almost all systems are, the BIOS-level PnP configuration takes place. The next thing that happens is a search for bootable devices. The order of this search is defined by the settings stored in CMOS memory, but is often `c:` (first partition on the first bootable hard drive), then the optical drive, followed by removable media, such as flash drives, and finally a bootable network card.

For each device in the list of potential bootable devices, the partition table is checked for the active partition. Floppy disks and the CD-ROM check only the first partition. For this partition, the first sector is read and checked for a boot loader. For modern Windows, the first sector is checked for the `bootmgr` file. When this file is located, it is executed. If it was not found on the first potential bootable device, the second and third devices are checked before reporting a boot failure.

## *Standard Boot Process for Windows*

Like with so many areas of the OS, each new version of Windows comes with changes to the core boot process. The major change implemented in Windows Vista is the introduction of the boot loader application; the configuration data is also stored in a different location. For Windows 7 and newer OSes, the boot loader is `bootmgr`. This process is used by current Windows OSes that have been released after Windows 7, so it is the same process that is used by Windows Server 2012 and newer server OSes.

## *bootmgr*

The boot manager (`bootmgr`) is responsible for reading the boot configuration data stored in the boot configuration database and displaying the boot menu. You will find a rescue copy of `bootmgr` stored on System Volume in the `\windows\boot\pcat` directory, but the copy that is used to boot your computer is actually found on the root of the hidden System Reserved partition that Windows creates when you perform your installation. This partition is not so much hidden, but rather not assigned a drive letter. The System Reserved partition is usually the first partition on your installation disk and will be marked as the active partition in the disk's partition table. The active partition is the partition where the POST process looks to locate the boot loader. If it is not the System Reserved partition, then it will be the `C:` drive.

## *Boot Configuration Database*

Rather than relying on boot configuration being stored in a single file, such as `boot.ini`, which was used in older Windows OSes, Microsoft now uses a Boot Configuration Database (BCD). This database stores more comprehensive information about the boot settings. If you are using a computer that supports EFI (Extensible Firmware Interface), the BCD is stored in the EFI System Partition. If you are using a computer that supports an IBM-style BIOS, the information is stored on the active partition in the `\Boot\BCD` file. If you need to make changes to this configuration, you can use the System Properties, `msconfig.exe`, `bootrec.exe`, or `bcdedit.exe`.

## *winload.exe*



If you choose to boot to Windows, the boot manager will transfer control over to `\windows\system32\winload.exe`, which is stored on System Volume. `winload.exe` — the OS boot loader — has one main job, and that is to load the Windows OS kernel (`ntoskrnl.exe`).

## *ntoskrnl.exe*

The main goal of the boot process is to get the OS kernel loaded and functioning. The computer has already given you a choice of OSes, inventoried the hardware, and is now ready to actually start loading the OS into memory. `ntoskrnl.exe` represents the first and most important step in this process. The OS kernel for Windows is responsible for all thread-level scheduling in the system. It plays a major control role, managing all other components on the system. Without it, there would be anarchy in the OS.

`winload.exe` proceeds to the path specified in BCD to locate `ntoskrnl.exe` in the `system32` folder. If the kernel is loaded, `winload.exe` proceeds to execute it. `winload.exe` will generate a missing kernel error message if it fails to locate the kernel. (Startup error messages are covered in Book 7, [Chapter 1](#).) After the kernel is running, `winload.exe` passes control of the system to it. There are several steps to the kernel load, starting with loading devices and then moving on to loading any system services. After the services are running, it loads the default shell application and user profile.

The default user profile is used to run the user logon process. At this point, the logon screen will tell you, `Press Ctrl+Alt+Delete to begin`. After providing logon credentials, that user session is discarded, and a new one is started for the new user.

## *The device load process*

All the devices to be loaded during the system startup are listed in the Registry. The Registry includes information about each device here:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\<device>
```

In this location, you can find several values that describe how the device will start up. These values are listed in [Table 6-1](#).

**TABLE 6-1 Device and Service Settings in the Registry**

<i>Value</i>	<i>Description</i>
Display Name	This string is used to display the name in areas of Windows, such as Device Manager or the Services administrative tool.
Error Control	This value configures how errors will be reported back to the OS. A value of 0 does not report any errors with the device back to the OS. A value of 1 reports errors normally. A value of 2 makes errors severe and will cause an automatic reboot of the computer to the Last Known Good Configuration. A value of 3 makes errors critical and will also cause an automatic reboot of the computer to the Last Known Good Configuration. If the Last Known Good Configuration is already used, severe errors will enable the computer to continue to boot, but critical errors will start the bug-check routine.
Group	Devices can be grouped. This is done mostly for dependencies. If any device in a group fails, dependent devices will not start.
Image Path	This is the path and name of the actual driver file that is used for the device or service.
Start	This identifies when the device will start up. The five start types are boot (0), system (1), automatic (2), manual (3), and disabled (4). Most devices have boot or system for a start value, but you might find a few set to automatic. Most services are set for either automatic or manual.
Tag	A Tag ID is assigned to the service when it is installed, but is not actually used by the OS.
Type	Identifies that type of service or device. All devices should have a value of 1. Service types should be 1 for kernel device drivers, 2 for file system drivers, 4 for arguments for an adapter, 10 for single process Win32 applications that follow the Service Control Protocol, and 20 for Win32 Services that can share their process with other Win32 Services.

## *The service load process*

All services that are to be loaded during the system startup are listed in the Registry. The Registry includes information about each device in the following location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\<service>
```

This is the same location used for devices. The biggest difference between devices and services is that devices map out to a physical piece

of hardware, but services are only software. The values for services are listed in [Table 6-1](#) in the previous section.

## *Loading the shell*

After processing all the device drivers, the user's shell loads. The application that makes up the shell is actually defined by a `shell =` line in `system.ini`, the default being `explorer.exe`. If the current shell ever crashes and is removed from RAM, `explorer.exe` will be loaded.

Explorer checks the Registry to see what desktop components are supposed to be displayed and then checks the

`HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices` key in the Registry to auto-start other applications. One of the services started at this point is the network service. When the network service is started up, you will be presented with a logon screen.

After loading the requested services, Explorer then executes any entries that it finds in the Registry in the

`HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce` key. Each entry under `runonce` is executed sequentially, waiting for each to finish before moving on to the next. When these are completed, Explorer then moves on to the run and load entries in `win.ini` to launch additional applications, followed by the run entries in the Registry, found in

`HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run`, and finally the Startup group from the Start menu, `Start ⇒ Programs ⇒ Startup`.



**TIP**

This process is almost identical for all versions of Windows that are based on Windows NT; this includes the latest versions of Windows. Microsoft has taken the opportunity to modify the boot process to make improvements to the overall OS loading system in the current OSes.



TIP

For information on editing the Registry, see the regedit.exe section in Book 6, [Chapter 4](#).

## *Managing Memory and Virtual Memory*

With the adoption of Windows NT–based OSes like Windows 7 and newer versions, you no longer need to worry about boot-time memory management because after the OS kernel loads, the memory structure switches to a flat memory model and implements a virtual memory structure.

As improvements were made in the field of RAM, and as computers with more and more memory continued to ship, software developers created applications that used the new memory. To make the entire process of managing memory easier, Microsoft decided to implement virtual memory for the Windows OSes. Virtual memory allows Windows to present a 32-bit virtual machine (VM) that contains 4GB of memory to applications running in the 32-bit Windows environment. When working with 64-bit Windows, 32-bit processes are still limited to 4GB of virtual memory, while 64-bit processes have a much higher limit. On 64-bit Windows 8.1 and newer versions, this limit is 128TB. The OS then used a Virtual Memory Manager (VMM) to control or manage the mapping of data between the virtual addresses used by the application and where the data was stored in physical memory. The VMM was also able to move data that was not being actively used in RAM to a file on the disk. The swapping of memory data pages to and from the disk file led to the file being named “swap file” in older versions of Windows and “paging file” in versions of Windows like Windows 7 and newer versions. The drawback in the system of swapping data shows up when an application wants to use data that is in the swap file because it then has to wait for the data to be retrieved back into RAM before it can be accessed.

Access speeds of hard disks are measured in milliseconds ( $10^{-3}$ ), and memory access is measured in nanoseconds ( $10^{-9}$ ). It should not be hard to guess that this means that when data has to be retrieved from the swap file on a hard drive, the process is extremely slow relative to retrieving it directly from RAM.



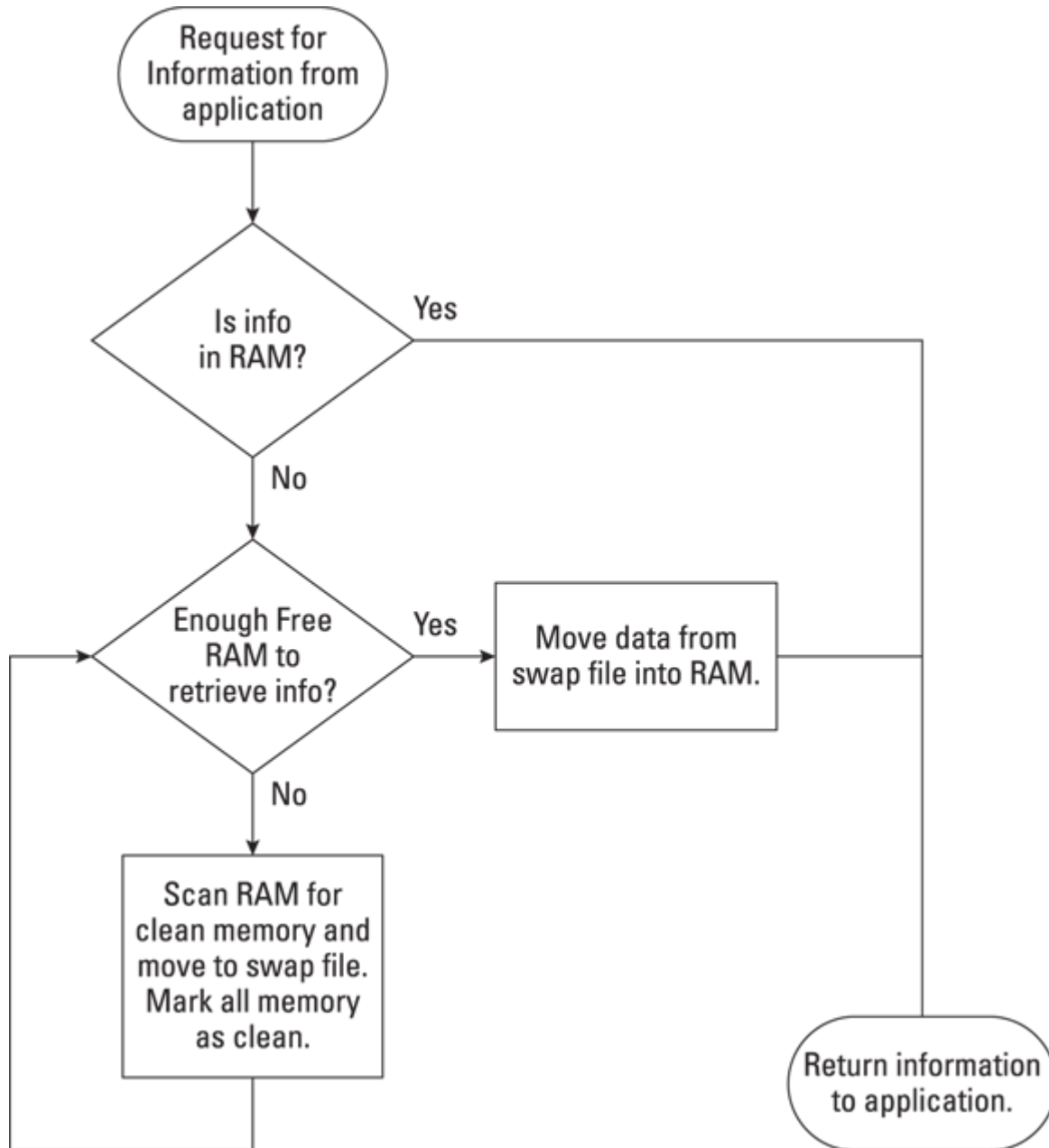
TECHNICAL  
STUFF

The VMM manages virtual memory addresses up to the virtual memory limit, such as 4GB or 128TB, and the mapping of those addresses to a physical location, either in RAM or on a hard drive. You should rely on using the paging file only when applications need a small amount of additional memory. Most OSes implement virtual memory and allow it to use swap space on a hard drive to allow applications with high memory requirements to function, but greater performance will be achieved by adding more physical RAM to the system.

When an application needs to store information to memory, it passes the request to the VMM. VMM stores the information in RAM but might move the information to the swap file on the drive later. The process for retrieving application data is illustrated in [Figure 6-1](#); the process looks like this:

1. When the application requests information, the VMM checks whether the information is in RAM.
2. If the information is in RAM, the information is simply returned to the application, and the process is complete.
3. If the information isn't in RAM, VMM checks whether there is enough space in RAM to retrieve the information from the swap file.
4. If there is enough space to retrieve the information, the information is retrieved from the drive, stored into RAM, and passed on to the application; and the process is complete.

5. If there isn't enough space to retrieve the information, VMM checks for memory locations that have not been accessed recently and passes them from RAM down to the swap file.
6. When enough information is moved to the swap file to make room for the requested information, that information is moved into RAM and then returned to the application.



**FIGURE 6-1:** The swap process.

A *clean* memory location in RAM is a location that has not been accessed since the last time the VMM marked it clean. If the memory location has been accessed with a read or write request, this location is marked as *dirty*. When looking for memory data to move to the swap file, each location is checked; if it is clean, it is moved to the hard drive, and if it is dirty, it is marked as dirty and left. If the first scan did not free enough RAM, an immediate second search for movable memory data is required, at which time any memory data that is now dirty is data that was accessed since the first scan, mere milliseconds ago. This algorithm is the Least Recently Used (LRU) algorithm, and it ensures that data that is actively used in RAM will stay in RAM.

The 32-bit versions of Windows allow a 32-bit memory space to be used. Rather than being able to use all 4GB ( $2^{32}$ ) of address space, only 2GB is configured by default for use with User Mode processes. User Mode processes are applications or processes that run on the computer. This includes server processes such as Microsoft Exchange and Microsoft SQL. The 64-bit version of Windows allows a 64-bit address space to be used by the VMM, which makes the limit 16EB ( $2^{64}$ ), but User Mode processes are limited to 8TB of space for running processes. The remainder of the space is used by operating system processes.



TECHNICAL  
STUFF

When running Windows 8.1 or newer OS on a 64-bit platform, the User Mode memory limit is increased to 128TB. This is the virtual memory limit, which defines the address locations that can be used, and which is different from the physical memory limit. The physical limit of 64-bit Windows 8 Enterprise is 512GB while 64-bit Windows 10 Enterprise is 6TB.

## Getting an A+

This chapter examines the process undertaken by the software on your computer during the boot process. The basic boot process for Windows

computers is discussed, as well as the differences between them.

Key points that you should remember about this chapter are

- » Virtual memory is managed by the Virtual Memory Manager, which presents a 4GB address space to 32-bit applications on the system. 64-bit applications on 64-bit OSes have a higher limit.
- » Virtual memory is made up of physical RAM and hard drive space in the form of a swap file or paging file.
- » The Windows boot process uses the `bootmgr`, `BCD`, and `winload.exe` files.

## *Prep Test*

**1. A user has a program that automatically starts when he logs into his computer. He would like to disable it. Where should he look for possible settings?**

- (A) `load` = lines in `win.ini`
- (B) The Startup group in the Start menu
- (C) The RUN key in the Registry
- (D) All the above
- (E) None of the above

**2. As part of troubleshooting the boot process on a Windows 10 computer, you are asked to identify the order in which files are processed. List the files from the left column in the right column in the order in which they are executed as part of the boot process. Not all files will be used.**



Choices	Answer
<div>ntoskrnl.exe</div> <div>ntldr</div> <div>winload.exe</div> <div>bootmgr</div> <div>boot.ini</div>	

**3. You have been called by a user to help resolve a problem with her computer booting. She has multiple hard drives installed in her computer. You need to find out why the wrong device is being used as a boot device. The search order for bootable drives is stored in which location?**

- (A) System BIOS
- (B) PNP Configuration
- (C) io.sys
- (D) CMOS Memory

**4. You are helping to bring an older support professional up to speed on the current Windows boot process. You have been asked to view the boot information that was formerly found in the boot.ini file. Where is this information currently stored?**

- (A) bootrec.exe
- (B) himem.sys
- (C) bcdedit.exe
- (D) BCD

**5. You are looking to export configuration information for multiple services so that you will have a backup of their configuration. Where should you look for the information that you want to archive?**

- (A) MFT
- (B) BCD
- (C) Pagefile
- (D) Registry

**6. How large is the memory address space that is presented in 32-bit applications running on a Windows 7 computer?**

- (A) 640KB
- (B) 1MB
- (C) 1GB
- (D) 4GB

**7. You are working with a user running 64-bit applications on a 64-bit version of Windows 7. The user is concerned about the application running out of useable memory on the computer. What is the limit of User Mode memory access on a Windows 7 computer?**

- (A) 128TB
- (B) 8TB
- (C) 4GB
- (D) 2GB

**8. What is the name of the file that Windows 7 uses to store memory data for the virtual memory system?**

- (A) Memory file
- (B) Swap file
- (C) Storage file
- (D) Paging file

## Answers

1. **D.** Automatic commands can be found in any of the listed locations (`win.ini`, Startup group, or the Registry). Review “[Standard Boot Process for Windows](#).”
2. The correct order of files used in the boot process is `bootmgr`, `winload.exe`, and `ntoskrnl.exe`. Check out “[Standard Boot Process for Windows](#).”

Choices	Answer
ntoskrnl.exe	bootmgr
ntldr	winload.exe
winload.exe	ntoskrnl.exe
bootmgr	
boot.ini	

3. **D.** CMOS memory contains the boot device order. *Take a look at “[The Power-On Self-Test \(POST\) Process](#).”*
4. **D.** With Windows Vista and newer OSes, you will find the information that was formerly found in the `boot.ini` file in the Boot Configuration Database (BCD). `bcdedit.exe` and `bootrec.exe` are tools for accessing the information in the BCD. `himem.sys` is an old memory management driver for MS DOS. *Peek at “[Boot Configuration Database](#).”*
5. **D.** The registry is where all service information is stored in the key `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\<service>`. *Examine “[The service load process](#).”*
6. **D.** The memory address that is present in each application or VM is 4GB in size. *Examine “[Managing Memory and Virtual Memory](#).”*
7. **B.** When running the 64-bit version of Windows lower than Windows 8.1, the User Mode memory limit is 8TB. It goes up to 128TB with Windows 8.1. *Refer to “[Managing Memory and Virtual Memory](#).”*
8. **D.** Windows 7 refers to the file used by virtual memory as a paging file or the page file. *Look over “[Managing Memory and Virtual Memory](#).”*

# Book 6

# Managing the Operating System

## Contents at a Glance

### Chapter 1: Loading and Configuring Device Drivers

[Loading Device Drivers](#)

[Changing Device Settings](#)

[Updating Drivers](#)

[Removing Device Drivers](#)

[Signed and Unsigned Drivers](#)

[Working with Plug and Play](#)

[Permissions to Install Drivers](#)

[Verifying Driver Installation](#)

[Device Driver Failure](#)

[Getting an A+](#)

[Prep Test](#)

[Answers](#)

### Chapter 2: Working with Applications

[Installing, Removing, and Repairing Applications](#)

[Getting the Most out of Multitasking](#)

[Running 32-Bit and 64-Bit Windows Applications](#)

[Running 16-Bit Windows Applications](#)

[Running MS-DOS–Based Applications](#)

[Windows Compatibility Modes](#)

[Application Install, Start, and Load Errors](#)

[Getting an A+](#)

[Prep Test](#)

[Answers](#)

### Chapter 3: Optimizing the Windows Environment

[Identifying Areas of System Bottlenecks](#)

[Using Monitoring Tools](#)

[Optimization Best Practices](#)

[Getting an A+](#)

[Prep Test](#)

[Answers](#)

## **Chapter 4: Using Windows-Based Troubleshooting Utilities**

[Understanding Operating System Utilities for Disk Maintenance](#)

[Working with Disk Management](#)

[Configuration Utilities](#)

[Getting a Handle on Diagnostic Utilities](#)

[Miscellaneous Utilities](#)

[Getting an A+](#)

[Prep Test](#)

[Answers](#)

## **Chapter 5: Scripting within the Operating System**

[Creating Your Files](#)

[Going Back to Basics with Batch Files](#)

[Working with VBScript](#)

[Getting More Power with Windows PowerShell](#)

[Shell \(.sh\) Script](#)

[Python Script](#)

[JavaScript](#)

[Commenting Your Code](#)

[Getting an A+](#)

[Prep Test](#)

[Answers](#)

# Chapter 1

## Loading and Configuring Device Drivers

---

### IN THIS CHAPTER

- » Looking at device driver requirements and installation
  - » Identifying and using signed drivers
  - » Working with drivers and diagnosing driver errors
- 

The United Nations' goal is for the nations of the world to work together and achieve common goals. They achieve this end by communicating with each other, but they first have to overcome the language barrier, which is done by employing hundreds of translators. *Device drivers* serve a similar role for computers that translators serve for the UN, converting information between the operating system and various pieces of hardware. Device drivers are responsible for establishing and maintaining communication links between an operating system and the various hardware devices on a computer. Each hardware device has its own language. The job of the device driver is to translate data from the device into something that the OS can understand, and then translate the OS data into something that the device can understand.

Even with the advent of Plug and Play, an A+ Certified Professional still needs to understand how drivers work and how to diagnose driver-related problems. Even though Plug and Play may allow for default drivers to be automatically selected and loaded, the entire process of managing drivers is not a hands-off process, and intervention will be required on many occasions.

## *Loading Device Drivers*

Because device drivers are so important, you should consider how device drivers are loaded onto your system. In the following sections, you take a look at loading device drivers for Windows. In [Book 3](#), you see how to configure the hardware to be added to a system; in this chapter, you focus on the software side of configuring these devices.



**REMEMBER** Because so many devices and drivers are floating around out there, the steps in this chapter for working with and managing drivers are necessarily broad and generic.

Drivers and their installation are tied to INF files, which contain installation instructions. There are several ways to install drivers with INF files:

- » Use Add a Device in the Windows Control Panel.
- » You might be able to use the INF files themselves.
- » You might have to load the drivers manually.
- » You might be able to install drivers directly through a setup program from the manufacturer, which can be used to install other software as well.



**REMEMBER** Before attempting device detection, ensure that the device is properly plugged in and powered; if not, the device will never be detected. And if the device is not detected, you have to manually load the drivers and configure the device. Loading drivers manually is discussed later in this section.





**WARNING** Some hardware vendors recommend that you copy their drivers onto your system before connecting the hardware to update the INF files to acknowledge that this hardware exists. This then allows the device to be properly detected when Windows finds it, allowing Windows to automatically load the drivers. This information is usually included with the vendor's Quick Install or Quick Start guide. In most cases, it does not really matter when the drivers are copied; if the drivers are not on your system, Windows will ask you where to find them.

By default, Windows uses Windows Update to locate and install drivers for devices that are installed into or connected to the system, which takes a lot of the work out of installing drivers. The settings for this behavior are found in the System Properties, as shown in [Figure 1-1](#). To locate these settings on Windows 7, follow these steps:

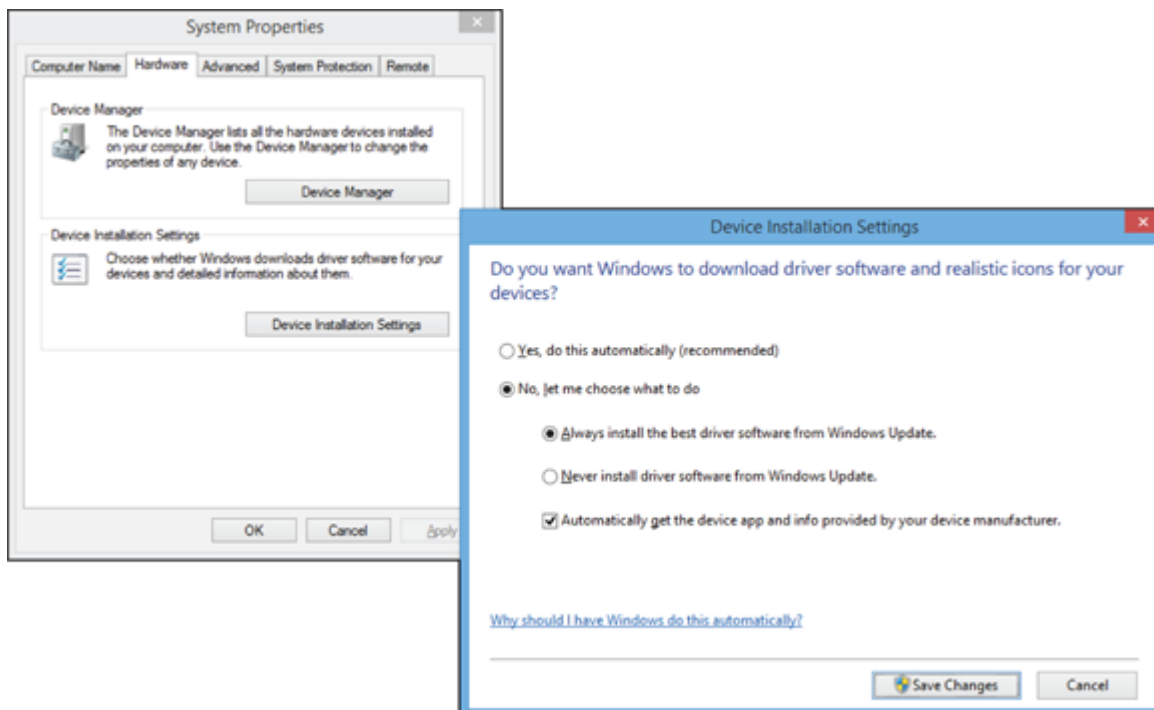
1. **Click Start.**
2. **Right-click Computer and choose Properties from the shortcut menu to open the System Properties dialog box.**  
On a Windows 8.1 computer, right-click Start and choose System.
3. **Choose Advanced System Settings from the navigation menu.**  
If you are prompted with a User Account Control dialog, choose Continue to proceed to the Systems Properties dialog.
4. **Click the Hardware tab and then click the Device Installation Settings button.**
5. **In the Device Installation Settings dialog box that opens (see [Figure 1-1](#)), select a radio button for how you do/do not want Windows 7 to check for driver updates for new hardware. You can**
  - Perform driver selection and installation automatically.
  - Have Windows automatically attempt to locate all drivers via Windows Update.

- Have Windows use Windows Update only when a local drive is not available for the device.
- Never use Windows Update for driver software.
- Optionally, Windows 7 can replace the generic icons representing the devices on your computer with more realistic icons by selecting the Replace Generic Device Icons with Enhanced Icons check box. With Windows 8.1, the option is to get the device app and information provided by the device manufacturer.



**REMEMBER** If you choose not to use Windows Update and if the drivers are not built into Windows or if they have not been installed, Windows will not be able to locate appropriate drivers for the device.

**6. Click Save Changes to close the Device Installation Settings choices, and then click OK to close System Properties.**



**FIGURE 1-1:** Using Windows Update for drivers can make it extremely easy to deal with new hardware.

To install a device driver on Windows using Add Legacy Hardware, follow these steps:

- 1. Start the device driver load process by launching the Add Legacy Hardware applet and follow these steps:**
  - a. Open the Control Panel by choosing Start or right-clicking Start (Windows 8.1).
  - b. Click Control Panel.
  - c. Click Hardware and Sound.
  - d. Click Device Manager.
  - e. Right-click the computer in Device Manager and click Add Legacy Hardware.

The Add Hardware Wizard starts.

- 2. When the Add Hardware Wizard starts, click Next.**
- 3. Indicate whether you already added the hardware to your system; then click Next.**

If you are adding a device, Windows performs a search of Plug and Play devices. The results of this search are displayed for you and include any unknown devices.



**TIP**

Because adding a device also includes a troubleshooting option, this is your opportunity to select a device already installed on the system that you would like to troubleshoot. If you select to troubleshoot a device, the next screen in the wizard informs you that when you finish the wizard, you will start the troubleshooter. The troubleshooter lets you set resource settings, such as IRQ and I/O addresses.

- 4. If the device that you need to load the drivers for is not listed, choose the option to Add a New Hardware Device at the bottom**

of the list; then click Next.

5. You have the option of letting Windows search for new hardware (shown in [Figure 1-2](#)), or you can select the hardware from a list.



**TIP**

If your computer appears to not be responding, give it some time to finish its detection process.

6. If no devices are found, click Next to manually choose a driver.
7. To install a device manually, first choose the hardware type (shown in [Figure 1-3](#)), and after you make your selection, click Next.

A screen listing manufacturers and models appears.

8. Choose the manufacturer and a model from that manufacturer and then click Next after making your selection.

If the device cannot be matched to known devices, you can click the Have Disk button to browse for or type the location of the device's INF file, as shown in [Figure 1-4](#).

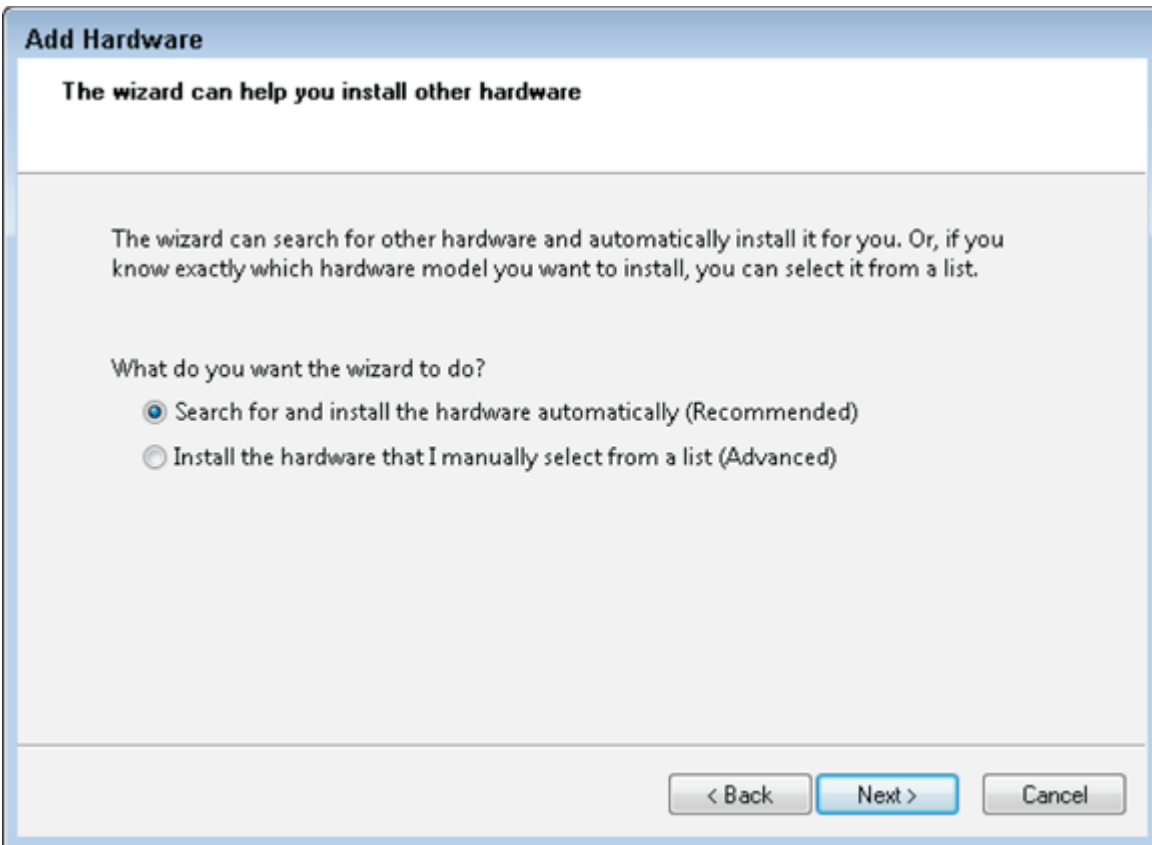
If Windows cannot detect the device settings for your device, it asks you to manually enter the settings for some or all of the hardware resources, which are I/O addresses, Memory, DMA, and IRQs.

You might be prompted for special device-related settings. If not, you should have a hardware installation dialog box on your screen.

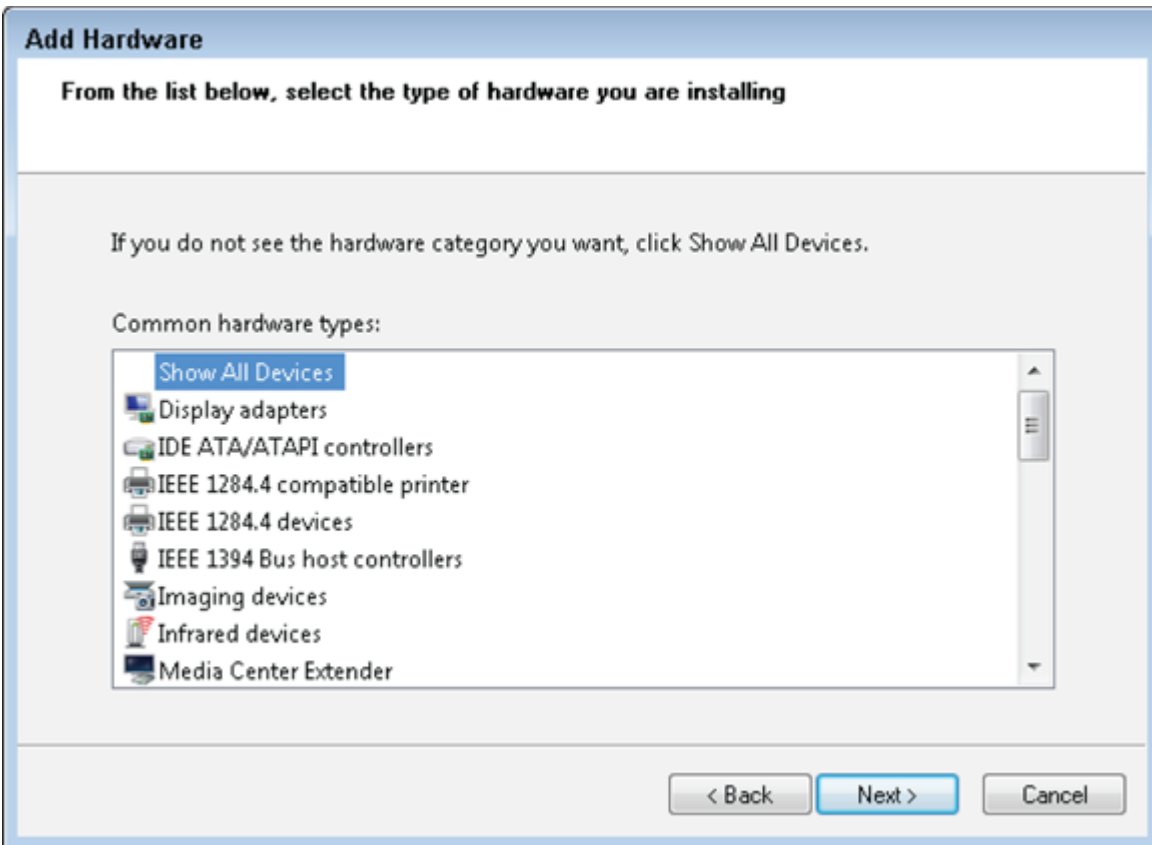
9. Click Next to start installing your hardware.

If Windows cannot locate some of the required files, it might ask you to insert a disk with the drivers on it or to locate the files that it needs.

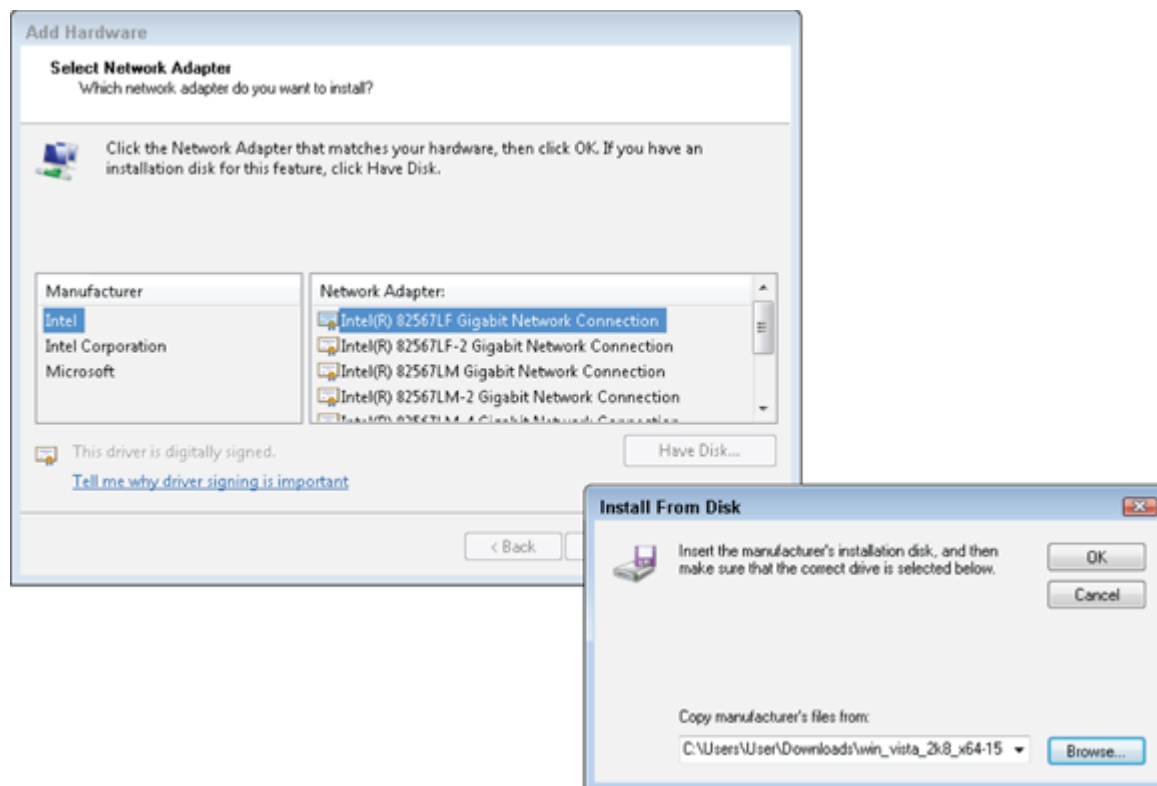
10. Click Finish when the installation is complete.



**FIGURE 1-2:** Plug and Play detection is used to initially locate all devices on your computer.



**FIGURE 1-3:** Choose the type of device you are installing so that you can look at a filtered list.



**FIGURE 1-4:** Device lists are listed by manufacturer to make locating devices easier.

If you need to manually adjust the hardware resource settings, you can change the settings for the device by using either the device's control panel (if one exists) or Device Manager.



**TIP**

Because control panels for each device are different, I look only at the Device Manager in this section.

To access the resource settings on Windows through Device Manager, use these steps:

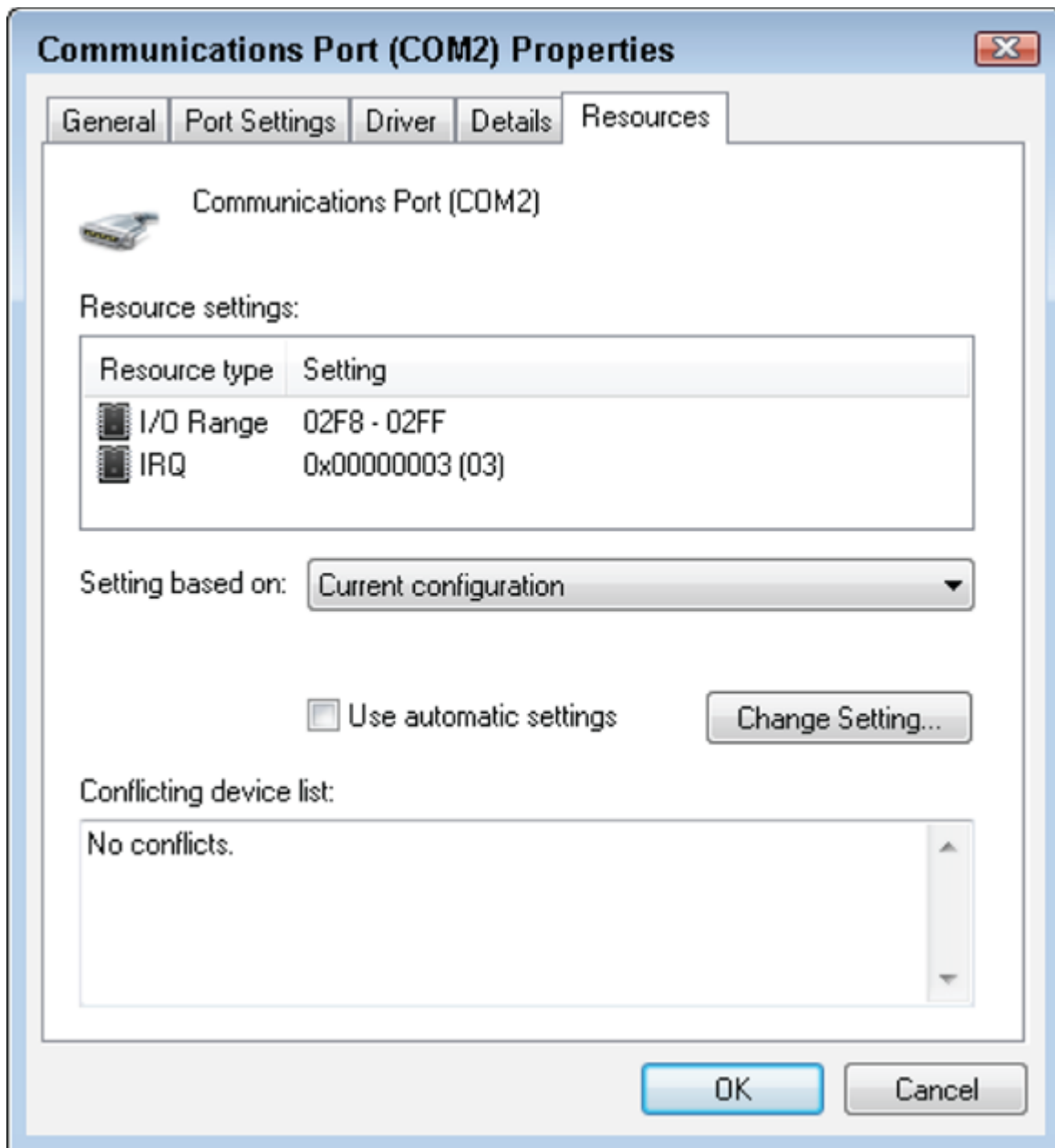
1. **Choose Start ⇒ Control Panel, click on Hardware and Sound, and then click the Device Manager link. (If you are using Windows 8.1 or Windows 10, right-click Start and choose Device Manager.)**

The Device Manager opens, and you can expand the device tree and select the device that you want to work with.

2. **When you find the device, right-click it and choose Properties.**

From the Properties window for the device, you can troubleshoot the device, examine driver details, change resource settings, and choose which hardware profiles will use the device.

3. Click the **Resources** tab to change the resource settings that are used by the device, as shown in [Figure 1-5](#).
4. After adjusting the settings, click **OK** to close the device properties dialog.



**FIGURE 1-5:** You might have to tell Windows what resources your device requires.





FOR THE  
EXAM

Device Manager is the main tool used for configuring and removing installed device drivers.

## *Changing Device Settings*

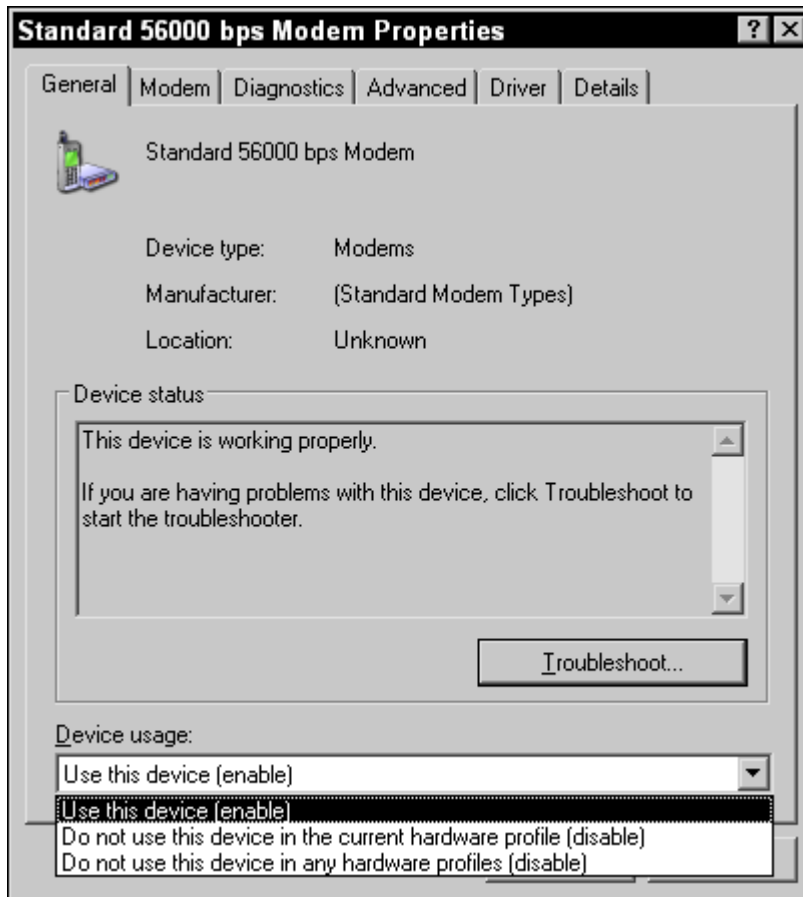
Regardless of how you install the drivers for the device, if Windows can't detect the settings for the device, you are prompted to specify IRQ, I/O, DMA, and memory resource settings. The prompt should only be necessary for non-Plug and Play devices. If you are not sure of the current settings for the device, confirm the settings by examining the hardware or by using the configuration utility that came with the device. A configuration utility should be included on the driver disk of any devices that support software configuration. If the device is configured for Plug and Play, you shouldn't have to worry about this.

For many devices, you can add drivers from the device's Control Panel applet, if there is one. This ability is not available for all devices but is available for modems and several other devices.

If you want to change the settings for a device that is installed on your system, you can use either the Control Panel applet for the device (such as Phone and Modem, Display, or Network) or Device Manager. Because each Control Panel applet is different, I do not go through each of them here, but rather show you Device Manager.

To access Device Manager in Windows 7, choose Start ⇒ Control Panel, click the Hardware and Sound link (opening the Hardware and Sound option), and then click the Device Manager link. You can also open the System Properties dialog box by right-clicking My Computer and choosing Manage, then clicking the Device Manager link in the Systems Tools section of the navigation menu. In newer Windows, right-click Start and choose Device Manager. With Device Manager open, expand the appropriate device tree until you see the device that you want to work with; then right-click the device and choose Properties. You can use the

Properties window to change the driver, and set resources for the device (see [Figure 1-6](#)). Based on how the driver was designed, you might not have a Driver or Resources tab and you will not be able to configure the settings on those tabs.



**FIGURE 1-6:** Device Manager is a powerful tool when it comes to device management.



ON THE  
WEB

Lab 1-1 guides you through examining the resources that are in use by your network card. In this exercise, you can use Windows 7, Windows 8.1, or Windows 10. Lab 1-1 can be found on the companion website at [www.dummies.com/go/aplusaio](http://www.dummies.com/go/aplusaio).

## *Updating Drivers*

From time to time, software vendors update their drivers, and you can choose to not update them, manually update them, or use Windows Update. When these drivers make it to the Windows Update website or Microsoft Update website, if you have upgraded, you can add them to your updates by choosing the optional hardware components. If you choose to update the drivers manually, right-click the device in Device Manager and choose Update Driver or click the Update Driver button on the Driver tab. Because some drivers do make it to the Windows Update website, the first question you will be asked when you choose to update your driver is whether you want to check Windows Update for copies of the drivers. If you choose not to use Windows Update or if there are no updated drivers on the site, you can still update them manually.

The next step in the update process is either allowing Windows to search automatically for updated driver software or having you manually specify a location for the drivers (“Browse my computer for driver software”). If you use the automatic method, Windows checks your currently installed INF files and the root directories of your removable media. If no matching drivers are found, you need to come back and choose Manual, which allows you to recheck the same paths as well as specify a directory in which to look for drivers. If all else fails, you can select “Don’t search. I will choose the drivers I want to install.” This option gives you a list of all drivers as well as a Have Disk button to load other drivers into the system. In most cases, you won’t have to use this screen. Just telling Windows to search a specific directory is usually enough for it to locate the correct driver for you.

Windows has streamlined the dialog boxes for this process, and will always check the Windows Update site as part of the automatic driver update process, unless you have changed the default Device Installation Settings, on the Hardware tab of System Properties (or Advanced System Settings).



**TIP**

Most of the Windows drivers will be updated when you apply an OS service pack. Microsoft often includes new drivers with the OS service packs.

## *Removing Device Drivers*

At some point, you might want to remove a device. The proper and clean removal of devices represents a large step forward in device management for the Windows OS. You can use Device Manager with all versions of Windows to cleanly remove devices and drivers. Device Manager allows you to select any installed device on your system and delete it. In addition to Device Manager, you may be able to use the individual device's Control Panel applet, such as the Network Control Panel applet.

To use Device Manager to remove a device from Windows, follow these steps:

1. **Choose Start ⇒ Control Panel, click Hardware and Sound, and then click the Device Manager link. (In Windows 8.1, right-click Start and choose Device Manager.)**
2. **Expand the hardware tree to locate your device, right-click the device, and choose Uninstall.**

You are presented with a confirmation dialog box.

3. **Click OK.**

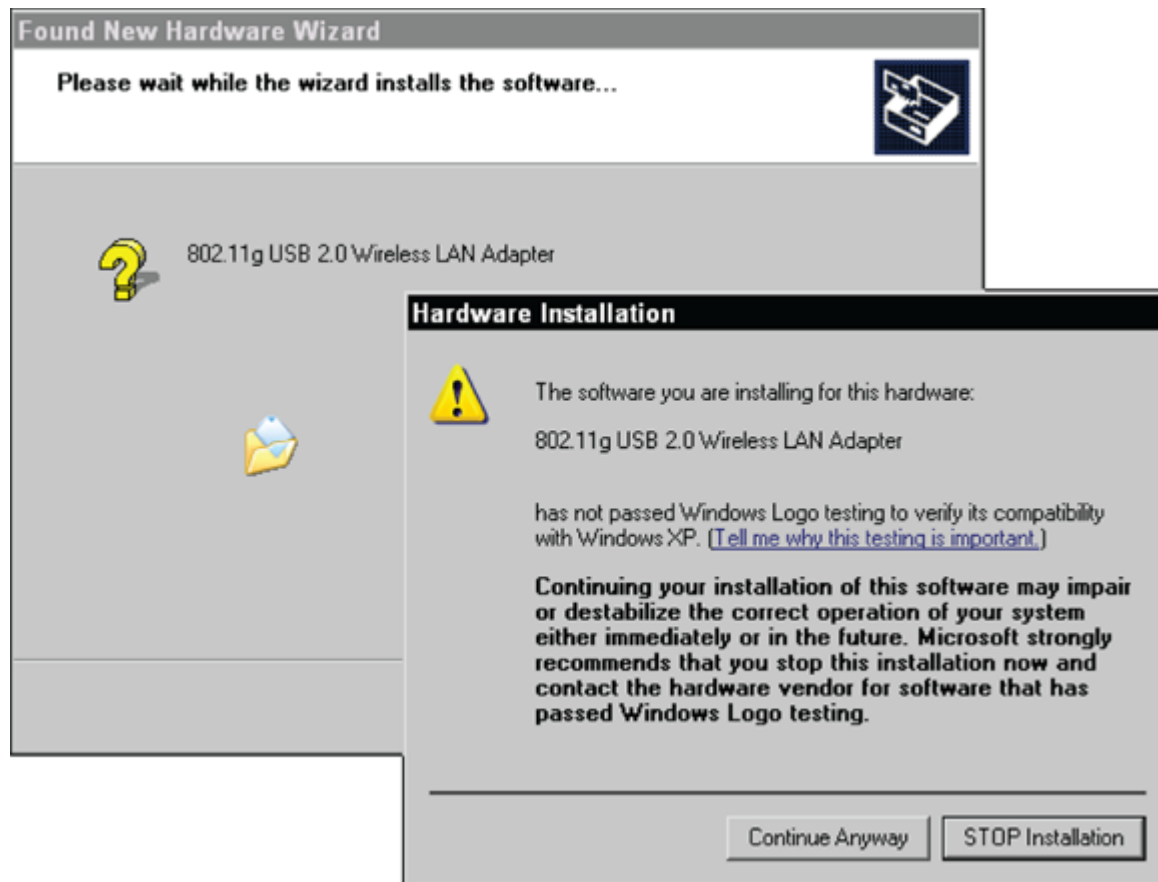
The device will be uninstalled.

Windows will (by default) unplug devices that you have removed, leaving drivers and settings behind for you in case you want to re-install the device. To see devices with Device Manager that have only been unplugged, choose View ⇒ Show Hidden Devices in Device Manager. This now shows all devices that have been installed on your computer, even if they are currently unplugged, and you can choose to remove them here and delete their drivers.

# *Signed and Unsigned Drivers*

*Driver signing* prevents installing unverified drivers on a system. Hardware vendors have to register with a certificate authority and verify their identity. Once they have accomplished this, they are able to sign the drivers which they created and generate a signature file. This signature file has a `.cat` extension and contains information about the original driver file to ensure that the driver was not modified since it was sent to Microsoft for Windows Update or delivered to you. When loading drivers, Windows checks for the existence of the signature file. If the signature is not available, you can configure what you want to have happen on the system. Your choices are

- » Ignore the missing signature and install the drivers.
- » Warn the user of the missing signature, but still give the option of installing (see [Figure 1-7](#)).
- » Block the installation of the driver.



**FIGURE 1-7:** Driver signing prevents installation of unwanted drivers.

Typically, the option to block unsigned drivers is enforced on high-availability workstations or servers. To modify these settings for Windows, you can

- » Choose on a per-boot basis.
  - a. *Press F8 at the start of the boot process.*
  - b. *Choose Disable Driver Signature Enforcement.*
- » Use `bcdedit.exe` to permanently disable driver signing by using the following command:

```
bcdedit.exe /set loadoptions DDISABLE_INTEGRITY_CHECKS
```



**REMEMBER** Any individual user can make his or her individual driver signing policy stronger than the administrator's defined system default.



**FOR THE EXAM** Driver signing is designed to increase system stability by requiring hardware manufacturers to validate their drivers with Microsoft.

## *Working with Plug and Play*

Thanks to Plug and Play, you have to do less work to add a device because device identification, driver selection, and hardware configuration are handled by Plug and Play (at least after the device has been added to the driver database). The Plug and Play specification says that a device should do the following:

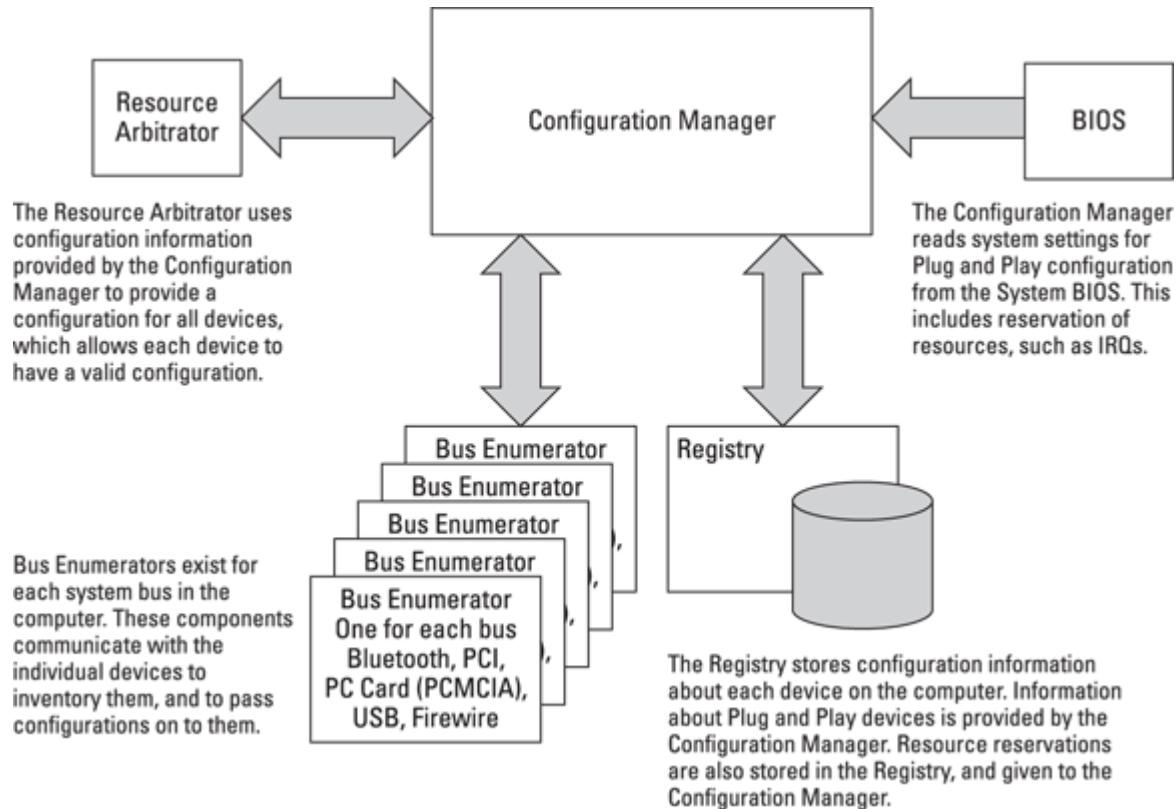
- » Be uniquely identified
- » State the services that it provides and the resources that it requires
- » Identify the driver that supports it
- » Allow software to configure it

The Plug and Play standard also requires that Plug and Play devices be backward compatible with non-Plug and Play systems — at least, that's the recommendation. All Plug and Play hardware should also be independent of operating systems that are installed on the system.

The Plug and Play process starts with the computer BIOS that supports Plug and Play. In addition, you also need an operating system that supports Plug and Play and Plug and Play devices. Current Windows OSes are Plug and Play-aware operating systems. The Plug and Play process contains three major components:

- » Bus Enumerator
- » Configuration Manager
- » Resource Arbitrator

[Figure 1-8](#) shows how these components fit together, and I discuss the whole Plug and Play process in the following paragraphs.



**FIGURE 1-8:** The Plug and Play concept is very simple in design.

At the lowest level in the Plug and Play process is the *Bus Enumerator*, whose job is to deal directly with individual devices. Each bus architecture in your computer has a Bus Enumerator, and the major bus architectures include PCIe, ExpressCard, SCSI, and USB. When a device is added to the system, especially in the case of PCMCIA devices, it announces its presence to the Bus Enumerator. The Bus Enumerator assigns an ID to the device, interrogates the device IRQ and I/O preferences, and possibly reconfigures the device based on requests from Configuration Manager.



The Bus Enumerator is called into action when a Plug and Play computer boots, and it has work to do whenever a device is added or removed from a particular bus. When the Bus Enumerator (and the rest of the Plug and Play system) is given a notification of device removal, it can prepare for it. For example, if you want to remove a PCMCIA Ethernet adapter, you can notify the Plug and Play system by stopping the device by clicking the PC Card icon in the notification area and choosing the Ethernet adapter.



FOR THE  
EXAM

Devices that can be removed or added to a running system are *hot swappable*. *Cold swapping* takes place when the machine is powered down, which is the case for most devices. ExpressCards support hot swapping, and some of the newer computers support hot swapping on the PCIe bus. Some manufacturers also use the term *warm swappable* to refer to components that can be replaced when the computer is in a sleep, standby, or other lower-power state.

The Bus Enumerator does *not* decide what resources the new device is going to use — that is the job of Configuration Manager. The Bus Enumerator passes all information about the device to Configuration Manager, which takes a look at all the resources required by all devices on the system. If multiple devices require the same resources, the Configuration Manager calls on the *Resource Arbitrator*, which evaluates which devices can operate at which settings and provides a solution in which all devices are able to use compatible settings.

After the Resource Arbitrator works its magic, a new resource configuration is passed to Configuration Manager. Configuration Manager accepts the new configuration; it contacts each Bus Enumerator and has the Bus Enumerator reconfigure any devices that require reconfiguration. So, although the Bus Enumerator doesn't decide how to reconfigure devices, it does actually carry out the reconfiguration of the devices.

All information about devices on your computer is written into the *Registry*, which maintains the hardware tree. Configuration Manager is responsible for writing the information into the Registry. In a computer

that supports the Plug and Play BIOS, the basic Plug and Play configuration is actually performed at the BIOS level. When the OS loads, it goes through the Plug and Play process and modifies any configurations that require modification.

If legacy devices (non-Plug and Play devices) exist on your system, resources are assigned to them first. This makes perfect sense because these devices cannot be reconfigured through the Plug and Play process. To ensure that the proper resources are allocated to legacy devices, you can reserve those resources in the system BIOS.

In most BIOS configurations, you have the option of reserving resources for non-Plug and Play devices. The settings in the BIOS tell you whether you are reserving resources for non-Plug and Play devices, reserving resources for legacy devices, or disabling resources. Those resources are not actually disabled, but their use by Plug and Play devices is disabled; legacy devices are still able to use these resources. The BIOS represents the best place to reserve legacy resources for this reason: It represents the first area where Plug and Play resources are actually assigned to devices.



**WARNING** Before changing any BIOS settings, consult your motherboard documentation. Incorrect modification of your BIOS can result in your computer not functioning.

Because legacy devices cannot be reconfigured through the Plug and Play process, they should always be allowed to use the resources that they require. In a perfect world, that would be all you need. Because we don't live in a perfect world, though, you must reserve resources. Reserving the resources for legacy devices at the BIOS level is more consistent for achieving a working configuration than allowing them to be reserved at the OS level.

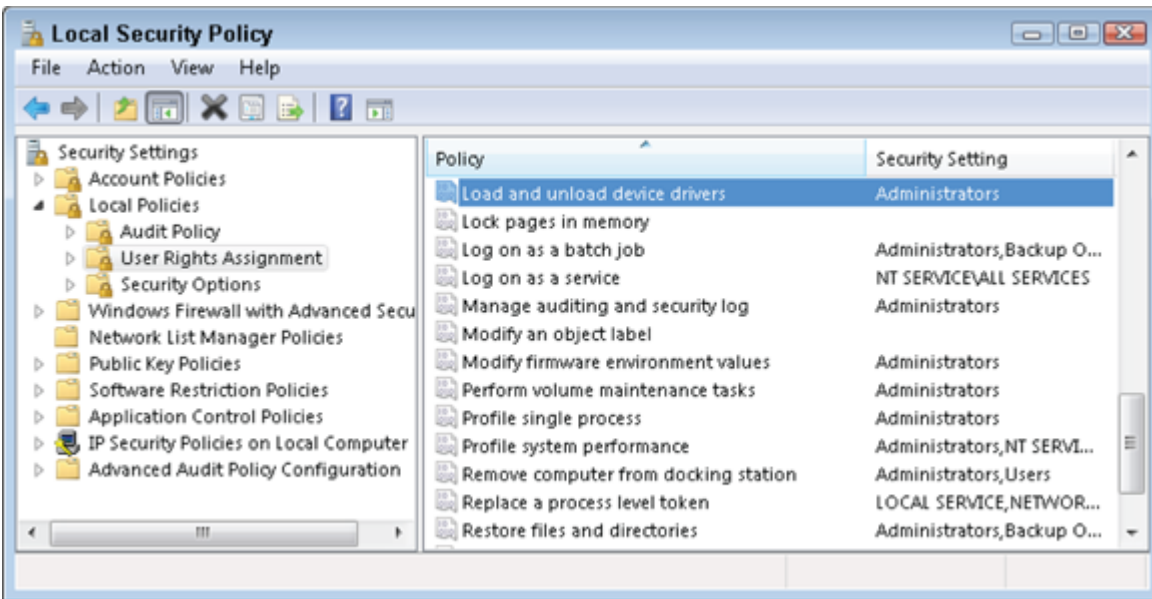
When Plug and Play systems first entered the market, they were plagued with difficulty. Much of this difficulty came from devices that were not fully Plug and Play-compliant or from non-Plug and Play-aware system BIOS, not to mention mixing Plug and Play and non-Plug and Play

devices together in a computer, which always causes additional problems and was often the case in early systems. Over the years, hardware and software manufacturers have learned a lot about how Plug and Play should and can work, and today Plug and Play is much closer to its ideal.

## *Permissions to Install Drivers*

To install drivers on a Windows computer, by default, you need to be a member of the Administrators group. In most cases, you do not want just anybody adding hardware devices to a computer and causing no end of problems for the people responsible for maintaining the computer. This ability to install the software for the device is controlled in the same way all rights on the computer are controlled, through the Security Policy. The computer policy can be changed locally. However, if the computer is part of Active Directory (AD), conflicting AD settings would override the local Security Policy. To view the active security settings on your computer and to see whether they are being overridden, you only have to look as far as the Administrative Tools by choosing Control Panel ⇒ System and Security.

In Administrative Tools, you will find the Local Security Policy application, which lets you see all security settings on your computer. To see the right to load and unload device drivers, expand the tree on the left to see Local Policies ⇒ User Rights Assignments. After selecting User Rights Assignments, you can browse the list on the right for Load and Unload Device Drivers. The Security Setting column tells you who has the permission, as shown in [Figure 1-9](#). To change the permission, double-click the security setting, and use the Load and Unload Device Drivers Properties dialog box to change the list of people who have permissions.



**FIGURE 1-9:** The Local Security Policy allows you to install device drivers.

## Verifying Driver Installation

To ensure that the drivers for a device are working properly, you should check three things:

- » **The device is listed in Device Manager, and it displays a “working properly” message.** If you see the Question mark category, you have some devices installed that do not have drivers.
- » **Make sure that the device is available to its own management or control software.** For instance, if a scanner does not show up in the scanning software application, that could be due to a faulty driver.
- » **Make sure that the device is yielding predictable results when used.** If not, the issue could be driver-related.



**REMEMBER** In most cases, if the drive is listed as working in Device Manager, the device driver is loaded properly for the device. So, the issues might actually be settings for the device or a hardware failure.

# *Device Driver Failure*

What do you do if a device driver does not work? This is a question heard many times by users with driver problems. The answer is, as always with computers, “It depends.” Some actions that you can take to deal with a malfunctioning driver include

- » Upgrading to a newer driver version
- » Removing the device
- » Rolling back drivers
- » Booting to the last known good configuration
- » Using restore points

If the driver is not working or if it has compromised the stability of the computer, you do have the preceding options. Issues with drivers could range from the driver just not working to the computer having a Stop event (blue screen error) during the boot process. In most cases, if the driver is just not working, look at how the device is connected to the computer and also examine any related components. For example, if the problem is with a USB device, are the rest of the USB components (such as the USB hubs and controllers) on the computer working?

After you verify this, and that the device is properly attached and powered, examine the driver version and its settings. Check for a newer (usually) driver or an older (rarely) driver that could fix your problem. Discussion boards often help diagnose driver-related issues, be they a version issue to settings related. In most cases, you should initially load the component with the latest driver available, which means ignoring the DVD that came with the device and going directly to the manufacturer’s website. If the device doesn’t work because of a hardware conflict, simply remove the device and replace it with a different manufacturer’s version. These hardware conflicts are very rare, but when they happen, you may have no choice but to replace with a different product.

Rather than just not working, the problem with the driver failure might be more prominent, such as a blue screen error during system boot. If that is the issue, your resolution is somewhat more critical. The first step is deciding what your immediate resolution needs to be. If it is to allow the computer to be usable and that the device was considered an extra feature, remove the device and look at adding and troubleshooting the device installation later. If it is to get the device working, you need to troubleshoot the device installation immediately. Your steps might vary some, but usually you want to do the following:

- » **Boot into Safe Mode to verify that base system files are still operational.** From there, you can remove or disable the device to allow the computer to boot. This can be done while leaving the device in the computer.
- » **If the error occurred as part of a driver update, choose the driver rollback option on the Driver tab of the device's Device Manager properties.**
- » **Download a newer version of the driver; you might be trying to load an older version of the driver with known problems.** The vendor's website will let you know whether newer versions of both drivers and firmware are available — and, often, what issues they corrected.



- » **WARNING** Risking the loss of configuration settings or files, the last two options are last-chance efforts to restore system stability in the form of booting to the Last Known Good Configuration or using a past system restore point. Because these two items return to a past point in time, you do run the risk of losing additional settings that you were not aware of. For more information about these two procedures, see Book 7, [Chapter 3](#).

In a perfect world, one of these fixes will work for you, and you won't lose any data or settings.

# Getting an A+

In this chapter, you look at general processes to load and configure device drivers. Specifically, you find out the following:

- » The driver installation procedures are found in INF files.
- » Drivers verified and signed include a `.cat` file, which contains the signature.
- » Plug and Play takes care of device resource settings for most devices.
- » Device Manager is the basic management tool for driver management.
- » Driver errors can be recovered by updating drivers, using Safe Mode, loading the Last Known Good Configuration, or restoring to a system restore point.

## Prep Test

- 1. A user has chronic issues with his computer. Your manager has asked you to visit the user and examine the device drivers. Device drivers are used to do what?**
  - (A) Provide power to the device while it is operating
  - (B) Act as a software interface between the operating system and the device
  - (C) Provide advanced configuration options for the device
  - (D) Steer the device to a new location on the computer
  
- 2. You have been looking for a driver for an old hardware device. You have not been able to find a signed driver and have only located an unsigned driver. What is the risk of using an unsigned driver?**
  - (A) Unsigned drivers are only reliable when using Windows XP.
  - (B) Unsigned drivers are missing their SIG files.
  - (C) Unsigned drivers are not backward compatible with older hardware versions.

- (D) Unsigned drivers cannot be verified for authenticity.
- 3. You are reviewing the Plug and Play process with a customer. Which of the following is *not* part of the Plug and Play procedure?**
- (A) Resource Arbitrator
  - (B) Dynamic Reconfigurator
  - (C) Configuration Manager
  - (D) Bus Enumerator
- 4. Which users on a Windows Vista computer have the right to load device drivers?**
- (A) Guests
  - (B) All users
  - (C) Administrators
  - (D) Power users

## *Answers*

1. **B.** Device drivers act as an intermediary between the operating system and physical devices. See “[Loading Device Drivers.](#)”
2. **D.** Unsigned drivers are missing their .cat files and their source and content cannot be verified. These drivers might work, but they are not verified. Review “[Signed and Unsigned Drivers.](#)”
3. **B.** The Dynamic Reconfigurator is not part of the Plug and Play procedure. Check out “[Working with Plug and Play.](#)”
4. **C.** Only members of the Administrators group have been granted the right to load and unload device drivers, by default. Peruse “[Permissions to Install Drivers.](#)”



## Chapter 2

# Working with Applications

---

### IN THIS CHAPTER

- » Identifying how 32-bit and 64-bit applications operate in Windows
  - » Diagnosing application install, start, or load failures with Windows
- 

If you work for a large contemporary company, then you may only have to deal with the newest of technology and may never have to deal with applications that are more than a few years old. If, on the other hand, you work for a consulting or service company that deals with small- to medium-sized businesses or organizations that focus on keeping technology spending down, then you will likely encounter a lot of old technology.

You never know when you are going to run into something old but still actively used. Recently I worked with a new customer with 20,000 computers. Due to a security requirement, this company still has a large number of users who are required to store data on floppy disks. Because you cannot purchase new machines with floppy disks, the company switched to using USB floppy disks (and you are probably not surprised to hear that the supply of those is pretty well dried up). Within the last 10 years, I have had two customers — a large grocery chain and a multi-site hospital — that both had current solutions that relied on ISA expansion cards. (ISA expansion slots are so old they are no longer covered in this book.) Once they exhausted all their suppliers of replacement motherboards, they both were finally forced to implement new solutions. This goes along with a packaging and plastics company that still used an MS-DOS-based program to control components of its manufacturing process, well after the release and demise of Windows XP.

To properly maintain and diagnose applications, an A+ Certified Professional must be able to manage the installation and removal of applications. In addition to these skills, this chapter also reveals the operating architecture in which applications run. Understanding this architecture allows the professional to diagnose problems quickly. You also examine the level of backward compatibility that is built into the modern Windows OSes, and you explore multitasking.

Given my history for dealing with people who hang onto and use old things, and that even the 32-bit version of Windows 8.1 supports MS-DOS and 16-bit Windows applications, I close this chapter with a few paragraphs on the old things, which if you are lucky, you will never need to know or use. If on the off chance you do need to support or deal with these devices, then this small background may help you.

## *Installing, Removing, and Repairing Applications*

Before you can work with applications on your computer, you need to install them. With the rate at which the computer industry changes, you cannot avoid the need to upgrade or remove applications on your computer as they become obsolete.



**TIP**

The terms *app*, *application*, and *program* are synonymous: They all refer to programming code that performs a function. In this chapter, though, I use the term *application* to describe the programming code that represents the functions you want installed on your computer — like a word processing application or a game. I use the term *program* to describe the programming code that allows you to install the application. And when referring to applications purchased from the Windows Store or applications that run on mobile devices, this is when the term *app* is used. (This chapter will not deal with apps, however.)

## *Installing an application*

Most applications come with an installation program that must be run to install the application. Some applications (say, the terminal emulation program PuTTY, from [www.chiark.greenend.org.uk/~sgtatham/putty](http://www.chiark.greenend.org.uk/~sgtatham/putty)) are actually stand-alone applications that do not require extra files and settings to be created on your computer, but these are rare. Most applications require several files to be installed and often require Registry entries to be created to hold the settings for the application. Because of the complexity involved in copying the files and creating the settings, you use the installation program to ensure that the application is installed properly. The application's developer decides the name of the setup program, which in many cases is `setup.exe` or `install.exe`.

Before installing a new application, you should ensure that your computer or device meets the hardware or system requirements related to drive space and RAM. If your device does not meet the requirements, you may find that the software will not perform as expected on the device. The setup program will verify that the hardware and system requirements are met before installing the program. In those cases when the requirements are not met, the setup program can prevent the application from being installed.

In addition to hardware requirements, the application may have similar requirements related to the OS installed on your computer or device. This may be the case if your device is running Windows 7 and the software requires that the OS is Windows 10 or above. In these cases, you may manually check to verify your OS is supported by the application, but the setup program may also prevent the application from being installed.

In most cases, a user needs administrative rights in order to install an application. When installing an application, you usually need to put files in or make changes to the following locations:

- » C:\Program Files
- » C:\Program Files (x86)

» C:\Windows

» HKey Local Machine\Software

All the places listed here have default permissions that restrict normal users from making changes to them. This by itself will be enough to prevent normal users from installing software. If the rights for these locations are modified, then a typical user would be able to install most software.

There are exceptions to user installation permissions. The Opera browser is one such example. When installing the Opera browser, if a user does not have rights to the previously mentioned locations, the setup program installs the files in the user's AppData directory and writes all registry entries to HKey Current User.

Controlling software installation and restricting users from freely installing software adds security to the computers you are managing. If users are able to freely install software, they may make poor choices related to the safety of the software they install, or they may choose to install software that is not compliant with your company's security policies. Poorly written software may inadvertently or purposefully cause performance issues on the device on which it is installed, or worse yet, it may over-saturate network connections and impact network performance. These impacts can have a detrimental effect on your ability to perform work. If these applications have a malicious intent, then it may have a dramatic impact on your personal or corporate data as well. Look ahead at implementing security in Book 9, [Chapter 2](#).

## WORKING WITH MSI FILES

Starting with Windows 2000, Microsoft created a new setup installation file. MSI files are associated with `msiexec.exe`, or the Windows Installer service. `msiexec.exe` is a generic application installer, and the Windows Installer service can be used to push applications out to computers on your network through Active Directory (AD).

The MSI file contains the installation script and, in most cases, also has a compressed copy of the files that need to be installed. If they are not stored in the MSI file, you will also have a CAB file.

Windows Installer or MSI installations have these benefits:

- Consistent user interface and command line interface
- Standard and easy way of customizing applications
- Diagnose and repair configuration problems at application runtime
- On-demand installation
- System-wide management of shared resources
- Restore the preinstallation state of a computer in the event of installation failure
- Elevated installation privileges

To install an MSI file, simply double-click it and follow any installation instructions.

Start looking toward Microsoft's next generation packaging with MSIX files, which are a combination of technologies, including .msi, appx, App-V, and ClickOnce.

Very few installation programs work in exactly the same way. In general, though, you are asked for the location where you want the application installed. Other options, such as whether you want to create a desktop shortcut to the application or whether you want a specific option to be enabled, are application specific.

There are several ways to install a program on your computer, but each basically runs the installer program. The following options are available from which programs may be installed:

- » Local Optical disc (DVD-ROM or CD-ROM)
- » Local Flash drive or USB device
- » Internet
- » Network

Windows 8 adds the option to also install software from the Windows Store. Windows Store applications differ from other applications as they are accessed via the Windows Store and are packaged in an .appx file format.

To install an application from the network, you can locate an install program on a network share, or you can use the Programs and Features Control Panel. To use the Program and Features Control Panel on a Windows 8.1 computer, use the following process:

1. **Right-click Start and choose Control Panel.**

2. **Click Get Programs.**

If the Get Programs link is not present, it is because your computer is not part of Active Directory.

The Get Programs screen will list any programs which are published through Active Directory or from other network sources, such as Microsoft's System Center Configuration Manager.

3. **Select a published application and click the Install button.**

The installation process for the application begins.



**TIP**

Many applications are distributed on CD-ROM, DVD-ROM, downloaded from a website, or a web service, like the Windows Store. For software shipped on an optical disc, when you insert the disc into your optical drive, Windows searches for an `autorun.inf` file and launches the program specified by the `autorun.inf` file. In most cases, the specified program is the application setup program if the application is not already installed. This AutoPlay feature of Windows makes installing applications even easier.

If you are using Windows 8.1, you have the option of installing an application from the Windows Store. These applications are published to the store by the application developer and are either free or available for online purchase. To install an application from the Windows Store, follow these steps:

1. **Click Start.**

The Start screen opens.

2. **Click the down arrow in the circle in the bottom-left corner of the screen.**

A list of all the applications installed on your computer appears.

3. **Click the Store icon in the S section of the listing.**

This launches the Store application. At this point you may use the Search bar in the top-right corner of the screen to look for an application or scroll through the collections, top charts, and categories of applications for the app you are interested in installing.



**TIP**

You may also find the Store icon pinned to the Taskbar or the Start screen.

4. **Select the application you want to install.**

The details regarding that application will be listed. If it is a purchased application, a Buy button appears; otherwise you will see an Install button.

5. **Click the Install (or Buy) button to install the application.**

If this is the first application you have installed, you will be asked if you want to set up a payment method for future purchases, even if the current application is free.

6. **Move your cursor to the top of screen to activate the Title bar, and click the X in the top-right corner to exit the Store.**

## ***Removing an application***

Most applications also provide a program to uninstall the application when you no longer want it on your hard drive. The path to the program and any switches that are required for it to function are usually stored in the Registry during the installation of the application.



**WARNING** Always use care when working in the Registry; improper changes can leave you in a position where you will be required to re-install the OS.

## UNINSTALL KEY AND THE REGISTRY

If an application uninstalls incorrectly or you would like to know what program is used to uninstall an application, the settings are stored in the Registry under the Uninstall key, which is found at:

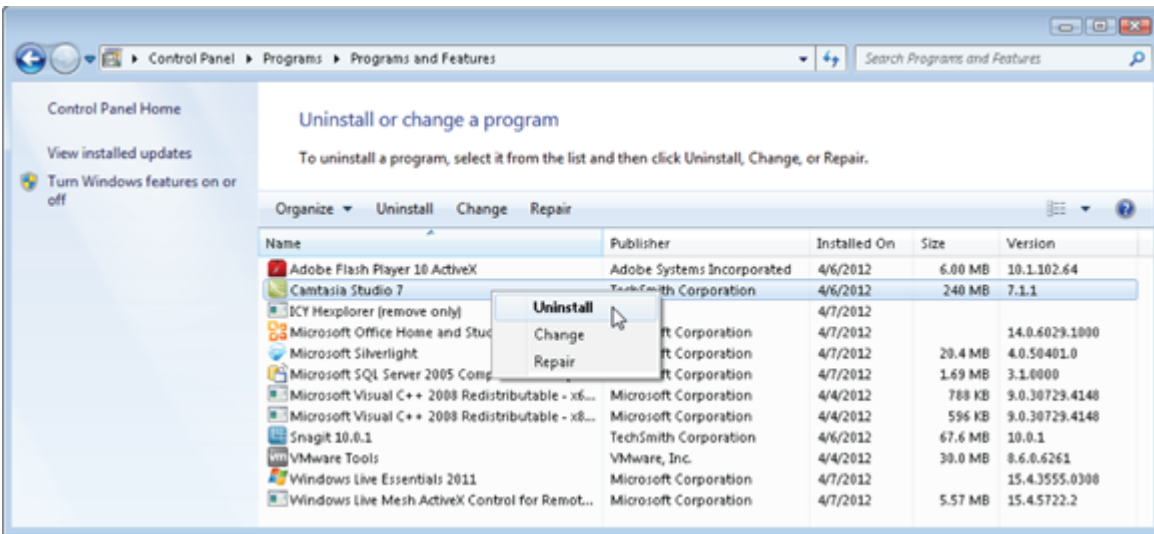
```
HKLM\Software\Microsoft\Windows\CurrentVersion\Uninstall\  
<Application_Key>\UninstallString
```

If the application was uninstalled but still shows up in the Add/Remove Programs Control Panel applet, you can delete the entire <Application\_Key> from the Registry.

With Windows, when you attempt to uninstall an application that is missing the uninstaller, it will ask whether you want to remove the entry from your Add/Remove Programs Control Panel applet.

The procedure to uninstall or remove a program from a Windows computer is very easy. After opening the Programs and Features Control Panel applet and clicking Uninstall a Program, select an installed application from the list, as shown in [Figure 2-1](#). You are provided details about that application, such as its size and when it was installed. In addition, you will see three buttons above the list of applications: Uninstall, Change, and Repair. To change the installed components of an application, click the Change button; to remove the application, click the Uninstall button. Some applications will have a Change/Remove button, which will then allow you to make changes to the list of installed components, or to remove the application; it uses the same program to accomplish both tasks. Windows looks up the name of the uninstallation program to run in the Registry and executes it.





**FIGURE 2-1:** The Uninstall options in Windows are more streamlined than previous versions.

Like the installation procedure, there is no set uninstall procedure, and it is left up to the software developer to design the uninstall routine. Some developers do an excellent job, and others do not. In the case of applications that do not uninstall properly, you might find the icons, files, or Registry entries still present after the uninstall program has completed. If that is the case, manually remove the leftover components.



**TIP** In many cases, applications are removed by using special options with the setup program that originally installed them. One nice feature of using the setup program is that many developers allow you to not only remove the application, but also to change the components that are installed.

## *Repairing an application*

From time to time something will happen to an application, be it user error or a system error. Whatever causes the problem is less important than the cure, and that is the application repair process. This process can easily be accessed via the Program and Features Control Panel using the following process on a Windows 8.1 computer:

1. **Right-click Start and choose Control Panel.**

**2. Click the Programs link.**

Programs opens and displays the Programs and Features link.

**3. Click the Uninstall a Program link.**

A list of programs that can be uninstalled or changed appears.

**4. Select a program that presents a Change option and then click Change.**

The application launches the setup program, which allows you to change, repair, or re-install the application.

**5. Follow the Repair Wizard options until the repair is complete.**



**FOR THE  
EXAM**

Make sure that you are familiar with the standard method of adding and removing applications from your system through the Programs and Features Control Panel.

## *Getting the Most out of Multitasking*

*Multitasking* is a computer's ability to balance the processing time given to multiple applications that are running at the same time. Multitasking comes in handy when running multiple applications at the same time.

The two basic types of multitasking are cooperative (which is very old), and preemptive. In this section, I discuss differences between the two types of multitasking; by the end, you should have a clear picture of which one is better.

### *Cooperative multitasking*

*Cooperative multitasking* means sharing time on the processor by cooperation. By its name, you would think cooperative multitasking is the better form of multitasking. This is probably because cooperation has always been thought of as a good thing. If you needed to get a job done (like building a house) and you had five people to help you, you could get the house raised quickly through teamwork and cooperation. This is a

good illustration of when cooperation works. However, if a couple of those people do not work with the rest of the team (they go to get more nails and never come back), their lack of cooperation slows down the process.

Likewise, with cooperative multitasking in the computer environment, a few programs that do not cooperate well with others can slow down the process. If you launch Microsoft Excel, for example, and start a large recalculation of the entire spreadsheet, Excel occupies 100 percent of the processor's time. At periodic intervals, Excel checks whether any other programs require processing time, at which time Excel turns control of the processor over to the other applications. Each application follows the same process that Excel does; they occupy 100 percent of the processor's time if needed, and give up control only when they reach their periodic interval for checking with the rest of the OS. If a program doesn't check with the other applications often enough, it is thought of as a *noncooperative program*. The big problem with noncooperative programs is that they can hog 100 percent of the processor time for as long as they want.

Cooperative multitasking was implemented to allow multitasking in a 16-bit Windows environment. Most of that environment was *single threaded*, meaning that only a single element (or thread) in the OS gives the processor instructions. As such, all applications have to work while sharing a single thread of execution. It might seem that cooperative multitasking is inefficient, but cooperative multitasking is better than no multitasking. However, because you are not likely to work with 16-bit applications, unless you are very unlucky, do not worry too much about cooperative multitasking.

## ***Preemptive multitasking***

Preemptive multitasking takes a different approach to multitasking in the Windows environment. With *preemptive multitasking*, the OS decides which applications get execution time. Preemptive multitasking is designed to work in a 32-bit *multithreaded* environment, in which applications have multiple execution threads, and the OS can manage

multiple threads issuing instructions to the processor or processors. Each thread of operation can run on any available processor in the computer.

Each application is given a certain percentage of execution time to use during each second. The OS then manages each process that accesses the processor. With the OS acting as the conductor, sharing the processor is more equal, with fewer conflicts. This does not mean that certain tasks do not attempt to run away with all the processor's computing time; it is just less likely to happen. Preemptive multitasking entered the Windows OS with the development of Windows NT, the grandfather of modern Windows OSes, and has been improving ever since.

All of what applies to 32-bit Windows applies equally to 64-bit Windows. To see this multitasking in action, find a single processor computer and an application that will use 100 percent of the CPU performing a function. Launch two to three copies of the application and watch the Processes tab in Task Manager. What you should see is that each copy of the application gets about the same amount of time on the processor, which shows preemptive multitasking in action. If you have multiple processors or cores in your computer, then to see this really work, you need to run many more copies of the application, two to three times the number of cores in your computer, to see the same sharing of processors on the computer.

## *Running 32-Bit and 64-Bit Windows Applications*

The 32-bit Windows applications are the ideal type of applications to run under a Windows 32-bit environment, and 64-bit applications are the ideal type of applications to run under a Windows 64-bit environment. All versions of Windows support 32-bit environments. All current Windows OSes have a 64-bit option when running on 64-bit processors. Because all these OSes are 32-bit or 64-bit in nature, it only makes sense that the applications that are run in these environments are also 32-bit or 64-bit. With that said, you should understand the benefits of running 32-bit and

64-bit applications and how those applications are executed in Windows environments.

## *Using 32-bit applications*

When Windows 32-bit applications entered the market, there were several benefits to running Windows 32-bit applications instead of 16-bit applications; and these were directly to showing the stability and power of the 32-bit Windows OS. These features are as meaningful today as when they were implemented. Features such as

- » Multithreading
- » 32-bit data transfers
- » Process isolation

One of the greatest benefits of 32-bit Windows applications is the ability to be multithreaded. *Multithreaded* applications run several threads of code concurrently. Each thread usually is assigned to a specific task. In the case of Microsoft Word, different threads can process typed characters, check spelling, or check grammar in your document all at the same time. If your computer has only one processor, only one task is actually performed at any given instance even though scheduling of all these different tasks is optimized. Even the latest couple of generations of phones have multicore processors, which really show off multithreaded applications, as each thread can be assigned to execute on a different processor. This not only optimizes the execution of the program but also evenly uses the processors. Be aware, not all 32-bit applications are multithreaded, and you will quickly see that in Task Manager as a single threaded application will heavily use a single processor or core, leaving the other relatively idle.

The 32-bit Windows applications work with data in 32-bit blocks, just as 16-bit applications work with data in 16-bit blocks. In any given clock cycle, a 32-bit application should be able to process more information than a similarly written 16-bit Windows application. In a perfect world, the speed factor of a 32-bit application would be twice that of a 16-bit application. Because we do not live in a perfect world, though, this

multiplier is not actually realized. Other factors that affect the performance of the application include how the logic in the code was optimized to allow these 32-bit blocks to provide better performance.

The 32-bit Windows applications also run with some level of isolation from other applications that are running on the system. This provides better stability for the applications that are executing.



TECHNICAL  
STUFF

When running 32-bit applications on a 64-bit version of Windows, the application runs in a 32-bit emulated environment called Windows on Windows 64, or WoW64. This allows the applications to run without any modifications. Applications that install into the C:\Program Files directory on a 32-bit Windows system will be installed into C:\Program Files (x86) on a 64-bit Windows system. The directory C:\Program Files is reserved for use by 64-bit Windows applications

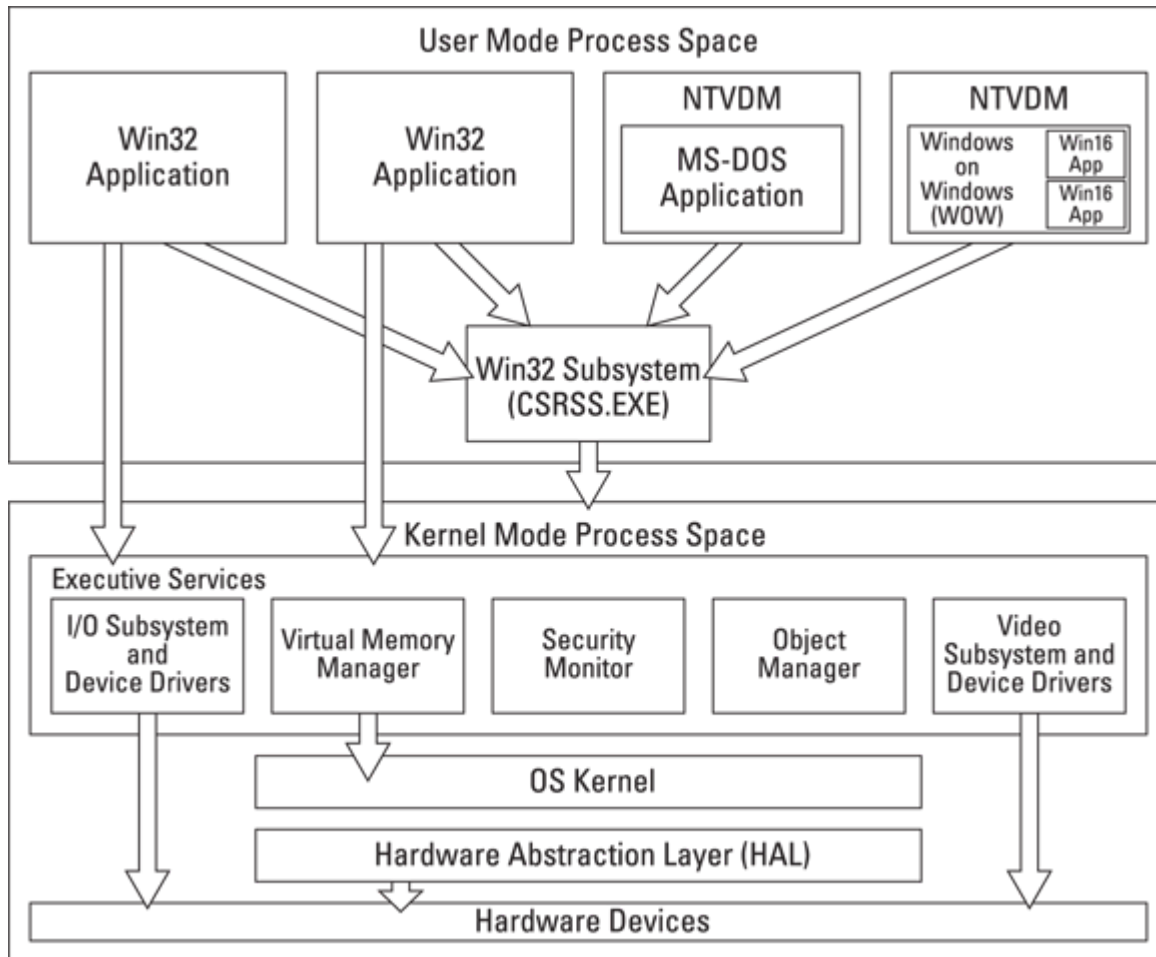
## ***Benefiting from 64-bit applications***

Microsoft now offers a 64-bit version of all current Windows OSes to run on computers with 64-bit processors. Most companies, unless they have a critical 32-bit application, have switched completely over to using 64-bit Windows on 64-bit computers. Some companies that implemented Windows 7 and Windows 8.1 have chosen to run 32-bit Windows on their new 64-bit computers to ensure compatibility with their current applications, but these companies are quickly becoming the exception to the rule. Like with 16-bit versus 32-bit applications, applications need to be rewritten and compiled to take advantage of this faster 64-bit architecture.

The 64-bit applications offer all the same benefits of 32-bit applications, such as multithreading. They have the additional benefit of 64-bit data transfers and processing units, which theoretically would provide a huge speed improvement over 32-bit processing.

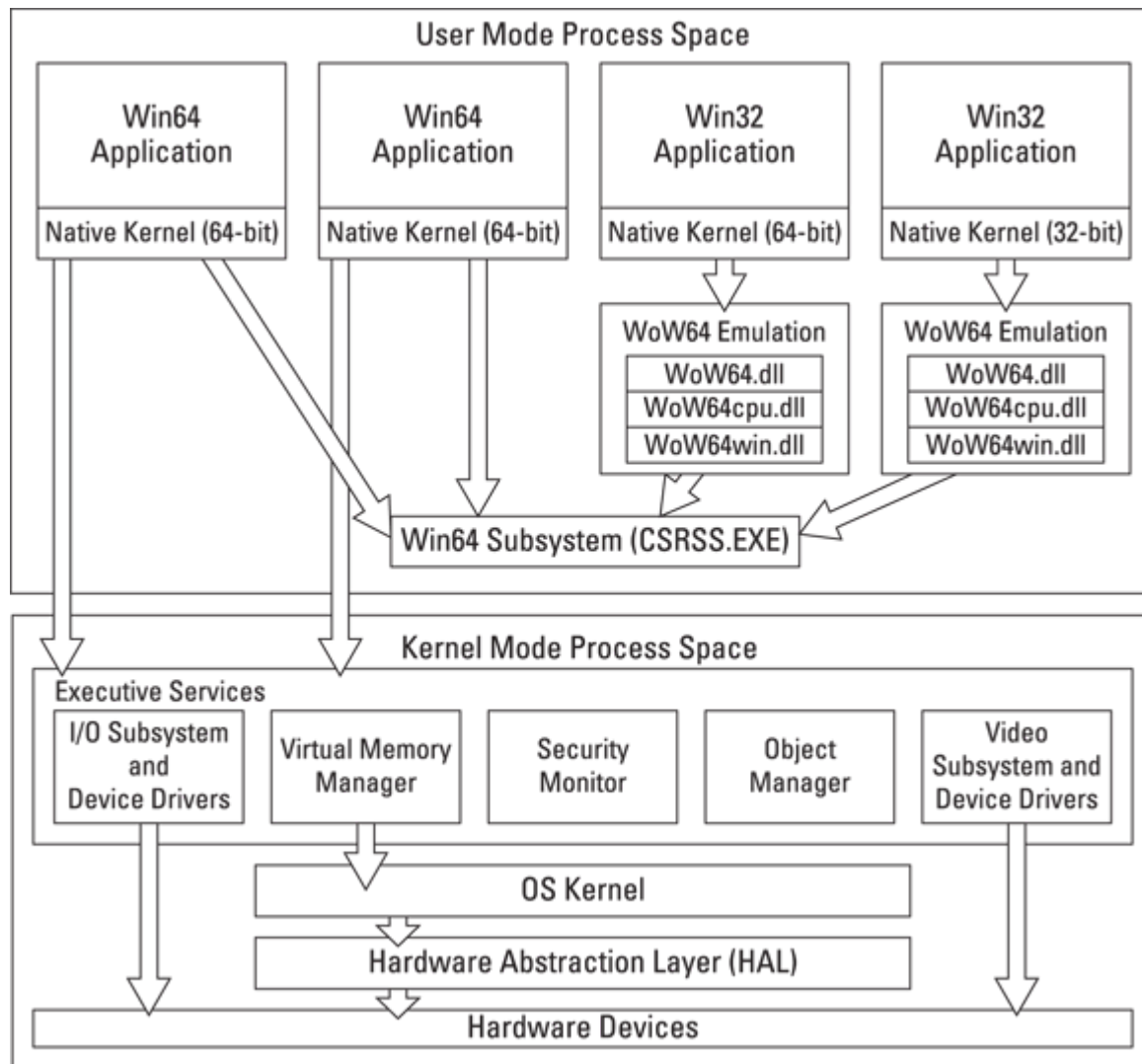
## ***Executing in the Windows environments***

The architectural diagram of 32-bit Windows is shown in [Figure 2-2](#), and all 32-bit versions of Windows use a similar architecture. Note that 32-bit Windows applications are executed as separate processes in the user mode portion of the OS, while 16-bit and MS-DOS applications run in an emulated 16-bit environment. This still holds true of any current 32-bit Windows OS, but it is very rare to find someone who needs support for 16-bit or MS-DOS applications.



**FIGURE 2-2:** 32-bit applications run in their own execution area in Windows.

The 64-bit architecture is similar to the 32-bit architecture, except it does not support 16-bit applications; it runs 64-bit applications in their own process space and runs each 32-bit Windows application in an emulated 32-bit environment hosted by Windows-on-Windows 64 (WOW64). This structure is shown in [Figure 2-3](#).



**FIGURE 2-3:** In 64-bit Windows, 32-bit applications run through an emulation layer.

In Windows, 32-bit and 64-bit Windows applications are executed in an area that is completely separate from where the OS executes processes. This provides the best stability for both the OS and the applications that are running in it, but does hinder some of the backward compatibility of the product. This does not mean that Windows is not backward compatible, but rather that it is *less* backward compatible than the previous generations. There have been attempts to increase the backward compatibility of the Windows product line, so applications that may not have worked with earlier versions of Windows may work under Windows 7, and applications that might not have worked under Windows 7 may work under Windows 8.1 or Windows 10.



Each 32-bit and 64-bit Windows application is given

- » **Its own address space to work with:** If an application hangs or crashes, the separate memory address space makes it easy to destroy or flush the entire memory that deals with that application.
- » **A separate message queue:** By having a separate message queue, if an application hangs or crashes, that halted application doesn't block the messages that are destined for other applications.
- » **The ability to own several threads that are preemptively multitasked by the OS:** Multiple threads per application allow the application to perform multiple operations at the same time.

## ADDRESS SPACE IN THE WINDOWS OS

The address space that the 32-bit OS works with is 4GB of address space, while the 64-bit architecture supports 16TB. This does not mean that you need 4GB of memory on the system to run the 32-bit OS; you need only as much physical memory as your applications actually use to store items. Physical memory is used only when an application stores something into a block of address space.

Picture each block of address space as a label, and physical memory as a wall of mailboxes. If I store something in a mailbox, I attach a label to that mailbox, representing what is stored there. When the application wants to store information, it might say, "Put this information in my address block 2045." The OS takes that information and puts it into any free memory block, and it then keeps track of mapping between those two locations for the application. When the application wants that information back, it says, "Give me the information in address block 2045," and the OS retrieves the information from where it was actually stored.

## *Running 16-Bit Windows Applications*

While it would be rare for you to encounter 16-bit applications in your technological journey, it doesn't hurt to have a little background. The 16-bit Windows applications were originally designed to run under Windows 3.x. Some of these applications look for specific components in the OS to function properly. To support 16-bit Windows applications, Windows

emulates the 16-bit Windows environment called *Windows on Windows*. (You can read about WoW earlier in this chapter.) The way in which this emulation is performed represents one of the big differences between versions of Windows.

The 16-bit Windows applications are single-threaded applications that actually share a single unit of execution with the 16-bit Windows environment. This is what I refer to earlier in the chapter as *cooperative multitasking*. The entire 16-bit Windows environment executes via a single processor thread. This thread is then shared among all 16-bit Windows applications running in the 16-bit Windows environment.

Within Windows, all 16-bit Windows applications are executed from within a 32-bit Windows *NTVDM (Virtual DOS Machine)*. This NTVDM is a complete, emulated DOS environment onto which a complete emulated 16-bit Windows environment is loaded. It is within this environment that 16-bit Windows applications are executed. Although this seems like a small point, it means that the entire 16-bit Windows environment that is implemented is contained within a newer Windows 32-bit or 64-bit environment. That makes the entire environment as safe and stable as any other Windows application running on the system.

An advantage to using current Windows environments is that 16-bit Windows applications can be run in separate memory spaces. When a 16-bit Windows application runs in a separate memory space, a new NTVDM is loaded along with a new WoW environment. The benefits of running applications in separate memory space are preemptive multitasking between applications and process isolation. It is important to note that 16-bit Windows applications cannot be run on 64-bit Windows.

As a CompTIA A+ Certified Professional, knowledge of these environments will allow you to address issues with applications and provide compelling reasons for late adopters to upgrade to the current Microsoft Windows OS.

# *Running MS-DOS–Based Applications*

This is the second piece of background information for dealing with technology holdouts, again, with luck, you will never have to deal with it. MS-DOS–based applications represent the oldest type of applications you are likely to run on your computer. MS-DOS applications are supported by 32-bit Windows. MS-DOS–based applications have always been designed to run alone on a computer. They expect to be the only application ever running on that PC, and as such expect to see certain things, like no Windows presence. Microsoft uses virtual machines to provide a unique environment for these applications. These virtual machines simulate all the hardware that would normally be found in a computer, including

- » Keyboard
- » Mouse
- » Monitor
- » COM ports
- » RAM
- » Disk drives

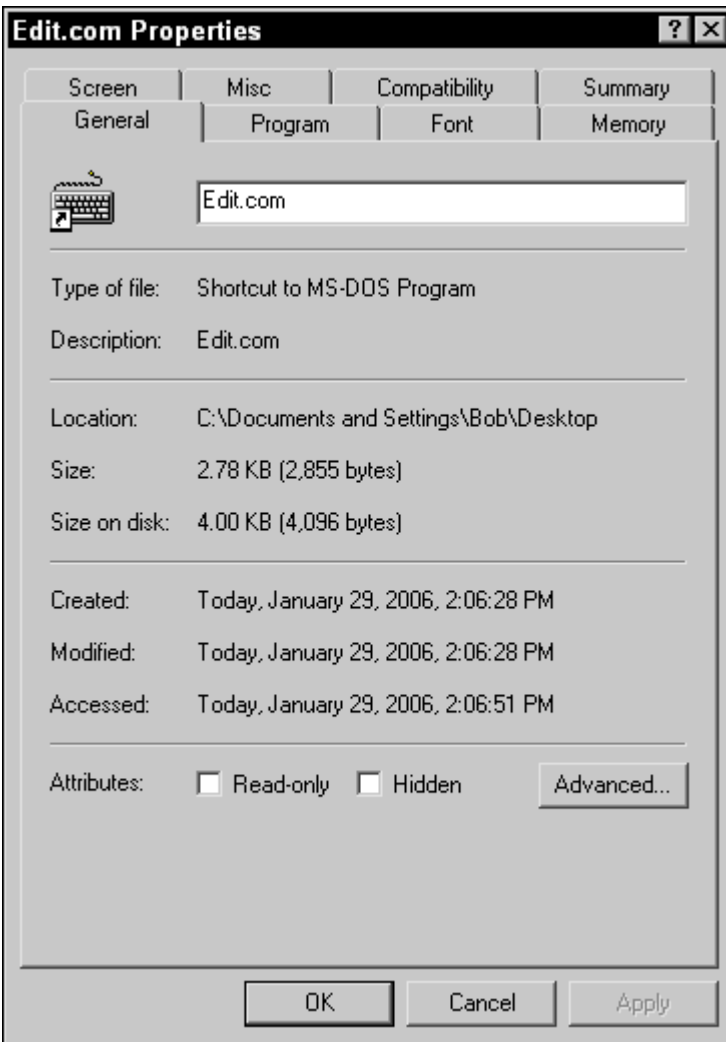
With all these components being virtualized, an MS-DOS–based application believes that it is running alone in a computer. The virtual computer’s settings can be modified through a *program information file (PIF)*, which I discuss in the next section.

## *Program information file (PIF) settings*

Every MS-DOS–based application that executes on your computer starts by configuring a working environment from settings found in a PIF. This is the case even if you are not aware that a PIF file is being used because a `_default.pif` file on your hard drive is used if no other PIF exists.

If you want to create a default PIF for a specific application, right-click the application and choose Properties. Even though there is not currently a PIF for the application, you will see all the PIF-related tabs, such as Screen, Memory, Font, and Misc. If you make any changes to the application settings on the tabs and click OK to close the dialog box, a file named `<application>.pif` is created in the same directory as the application executable. This PIF then becomes the default PIF for that application because it is in the same directory as the application and is named `<application.pif>`. Unlike most files, the `.pif` extension stays hidden, even if displaying file extensions is enabled.

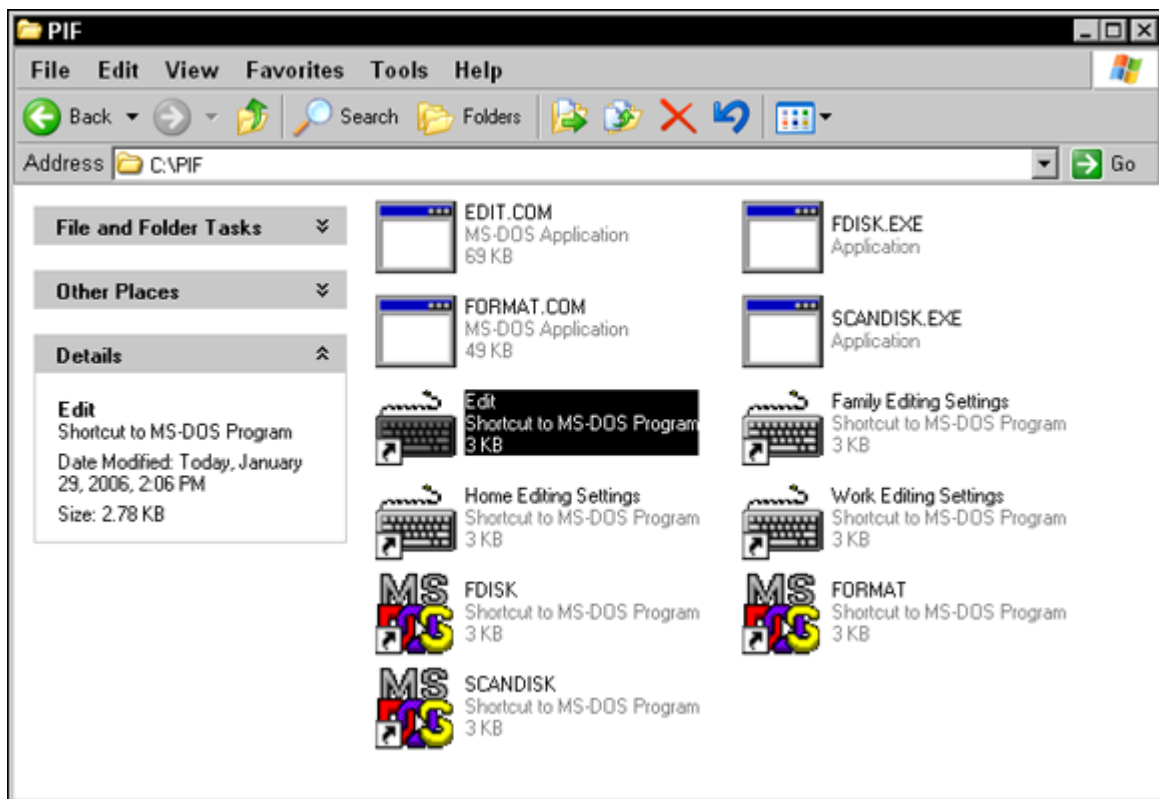
You can discern a PIF file by viewing the properties of the file (right-click it and choose Properties). The file type will be Shortcut to MS-DOS Program; and the Font, Memory, Screen, and Misc tabs are specific to PIF files, as shown in [Figure 2-4](#). At any time after closing the dialog box and the default PIF has been created, you can make changes to it by right-clicking either the application or the PIF to bring up Properties; either action allows you to edit the settings. Even though you can access the settings through the properties of the application, you are really editing the PIF.



**FIGURE 2-4:** PIFs have several tabs that contain settings for a simulated MS-DOS environment.

You might also be confused by the fact that a PIF for an application looks exactly like a shortcut for a LNK file. [Figure 2-5](#) shows a series of PIFs created for four MS-DOS–based applications. Notice that the first four icons in the window are MS-DOS application icons, and the last three icons are the default PIFs for the `fdisk.exe`, `format.com`, and `scandisk.exe` applications. In addition to the default PIF, `edit.com` has three additional PIFs that have been created for it (the keyboard-looking icons in the middle of the window). Each `edit.com` PIF can have its own unique settings. To access the settings for a PIF, right-click it and choose Properties. The Properties window of a PIF contains seven tabs:

- » General
- » Program
- » Font
- » Memory
- » Screen
- » Misc
- » Summary



**FIGURE 2-5:** Each PIF for a common application can contain unique settings.



**TIP**

You should always exit your MS-DOS application from within the program, using whatever commands or options are required.

Unlike Windows programs that have a standard Exit in the File menu, MS-DOS applications usually have their own special commands for exiting or closing the application, such as key combinations using CTRL or ALT, and Q, X, or W.

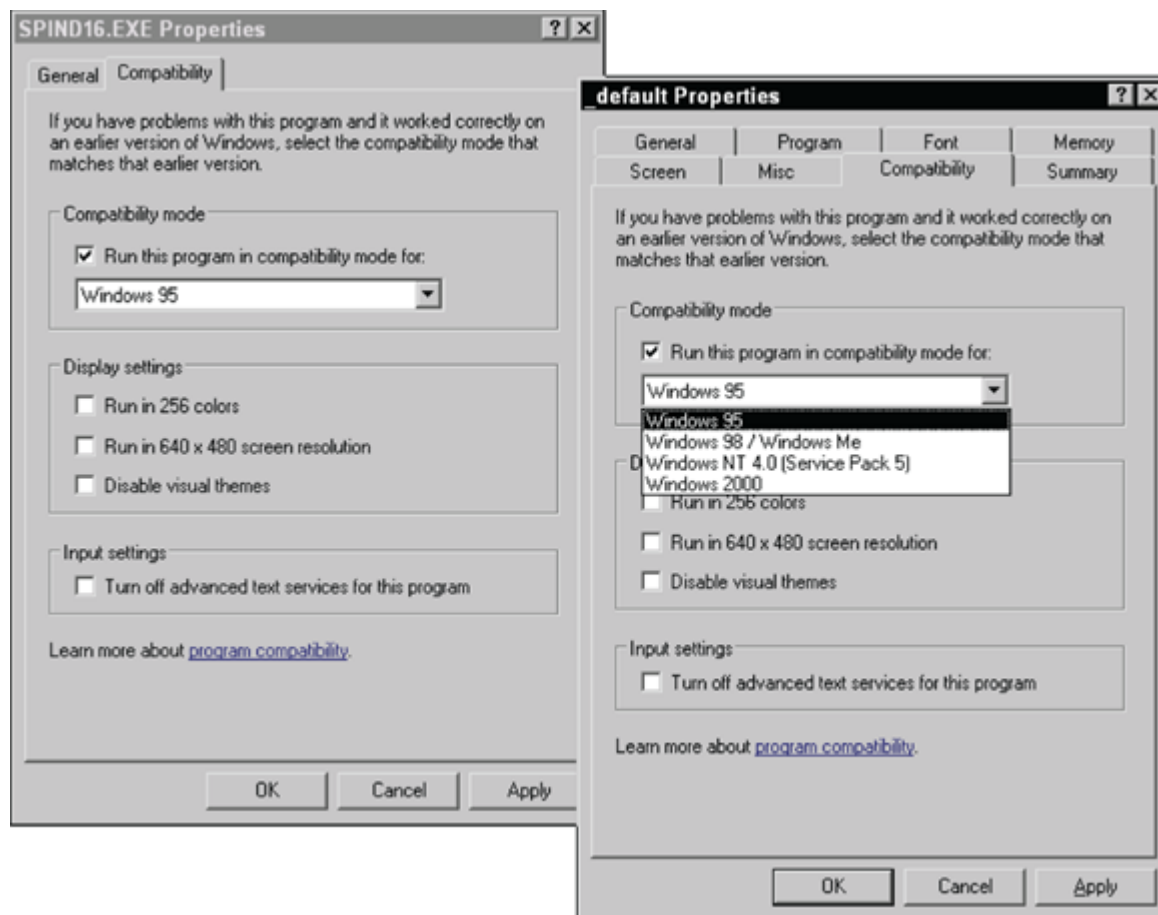
## *Understanding incompatibilities*

When you examined 16-bit Windows-based applications earlier in this chapter, you looked at potential incompatibilities that could arise from direct hardware access. The same incompatibilities apply to MS-DOS-based applications. If your application attempts to make direct hardware calls instead of standard MS-DOS-based system calls, it will not function under modern Windows OSes. Modern Windows OSes attempt to be backward compatible, but not at the risk of OS stability. Basically, if you have an application that makes direct hardware calls, it will not work under the newer Windows OSes.

## *Windows Compatibility Modes*

Microsoft takes backward compatibility seriously, so many applications written for their first OS (MS-DOS) or earlier versions of Windows will work with current versions of Windows with a few minor tweaks.

Microsoft has provided a new set of options to aid with backward compatibility for applications that are not included with the OS. These features are found on the Compatibility tab in the Properties dialog box of the executables, shortcuts, and PIFs. Compatibility settings for an old Windows application are shown in [Figure 2-6](#).



**FIGURE 2-6:** The Compatibility settings for an application.



**REMEMBER** These options are designed to be used with locally installed applications. You can use them with applications from CD-ROMs or from a network drive, but the settings will not be saved.

Because many applications have been written to take advantage of specific features found in various versions of the OS, the Compatibility Mode section allows you to emulate the following OSes:

- » Windows 95
- » Windows 98/Windows Me
- » Windows NT 4.0 (Service Pack 5)
- » Windows 2000



» Windows XP (Service Pack 2)

This does not emulate the entire OS, but rather disables some newer APIs (application programming interfaces) and emulates some older ones, thereby improving compatibility.

Windows 7 adds the following OSes to the Compatibility Mode section:

- » Windows XP (Service Pack 3)
- » Windows Vista
- » Windows Vista (Service Pack 1)
- » Windows Vista (Service Pack 2)

Windows 8 adds Windows 7 to the Compatibility Mode OS list, and Windows 8.1 adds Windows 8 to the Compatibility Mode OS list.

Another common problem revolves around screen settings. Many times, I have had to change my screen resolution or color depth to run a specific application (and then reset it later). The Display Settings section allows you to automatically change the display settings for the application to one of the following settings:

- » Reduce color mode to 8-bit (256) colors
- » Reduce color mode to 16-bit (65,536) colors
- » Run in 640 x 480 screen resolution
- » Run this program as an administrator
- » Disable visual themes
- » Disable desktop composition
- » Disable display scaling on high DPI settings
- » Enable this program to work with OneDrive files



**TIP**

If you have an application that has problems displaying menus or toolbar buttons, you can attempt to use the Disable Visual Themes setting. This removes the modern rendering of buttons, with the Windows smoothness, drop shadows, Aero desktop, and so on.



**TIP**

Most of the settings that can be adjusted or disabled on the Compatibility tab can also be changed elsewhere, such as the Performance Options, on the Advanced tab of the System Control Panel, which will change the setting globally for the computer.



**FOR THE  
EXAM**

If you have an old application that will not run properly on Windows, do not forget about the Application Compatibility Settings.

## *Application Install, Start, and Load Errors*

Many Windows application errors are related to permissions to the file system when using NTFS and the Registry. Starting with Windows 7, the default permissions restrict changes to files, addition of files to specific directories, and changes to portions of the Registry. In addition to these restrictions, many applications that attempt to directly access hardware will fail. If the application is a modern 32-bit or 64-bit Windows application that is supposed to work with Windows 7, most installation errors can be traced to not meeting either the minimum installation requirements or permissions.

Microsoft has made these permissions changes to prevent most users from being able to install their own applications and make unauthorized changes to the OS. One way to see whether the problem is with a user installing or launching an application is to temporarily add the user to the local Administrators group and see whether the problem is resolved. If that resolves the issue, you know that the problem is related to permissions to one of these locations.

If you can't get permissions information from the application vendor or can't grant the user elevated group membership, the Microsoft Sysinternals (<http://technet.microsoft.com/en-us/sysinternals/default.aspx>) Process Monitor utility can help you identify the permissions changes required.

## *Getting an A+*

This chapter examines application management from installation to execution. The following points are covered:

- » The application support architecture of 32-bit Windows and 64-bit Windows when it comes to running and supporting applications.
- » There are core architectural differences between 32-bit and 64-bit Windows. Support for applications differs based on the architectural differences of the OSes.
- » The new application compatibility features in Windows allow it to support a wider range of older Windows applications.

## *Prep Test*

**1. You are trying to resolve application installation issues when attempting to install an application on a computer under a user's (Bob's) rights. What Windows locations could be causing an issue with installation?**

- (A) HKey Current User\Software
- (B) C:\Users\Bob\AppData

- (C) C:\Program Files
- (D) C:\Users\Bob\Downloads

**2. You have an application that has very large memory requirements. How large is the memory space that each 32-bit Windows application has to work with?**

- (A) 16MB
- (B) 1GB
- (C) 2GB
- (D) 4GB

**3. To support your company's 16-bit custom application, you need to select an OS for the computers that will be running the application. Which of the following operating systems support 16-bit Windows applications? Choose all that apply.**

- (A) Windows 7 32-bit
- (B) Windows 7 64-bit
- (C) Windows 8.1 32-bit
- (D) Windows 8.1 64-bit
- (E) MS-DOS

**4. You are assisting a user with an application that is constantly crashing when it is launched. What effect does a 32-bit Windows application have on the rest of a Windows system when it hangs or crashes?**

- (A) It halts 32-bit Windows applications that are running on the system.
- (B) It causes a panic in the NTOSkernel.
- (C) It results in a halt screen or blue screen (BSOD) error.
- (D) It has no effect on other applications.

## *Answers*

1. **C.** Windows applies permissions to HKey Local Machine, C:\Program Files, C:\Program Files (x86), and C:\Windows, and these permissions will prevent ordinary users from installing software. Check out “[Installing an application.](#)”
2. **D.** Each application or VM runs in a 4GB memory space. Take a look at “[Running 32-Bit and 64-Bit Windows Applications.](#)”
3. **A, C.** Only Windows-based OSes can run Windows-based applications, and only Windows 32-bit OSes are able to run 16-bit Windows applications. Peek at “[Running 16-Bit Windows Applications.](#)”
4. **D.** When a 32-bit Windows application crashes, it has no effect on other applications running on the system. Study “[Executing in the Windows environments.](#)”

# Chapter 3

## Optimizing the Windows Environment

---

### IN THIS CHAPTER

- » Optimizing operating systems by modifying virtual memory settings
  - » Using utilities to monitor and identify optimization areas
  - » Optimizing hard drives and temporary files
  - » Improving performance by turning off OS features
  - » Managing services and startup of applications to optimize system performance
- 

Few things in life are perfect, and if you put them on a scale from perfect to lousy, most things fall somewhere in the middle. Computers play a part in my life, and I can safely say that they are not perfect, especially when dealing with speed and performance. I regularly work with other people's computers and find the responsiveness of many computers far less — very far less — than perfect. Over time, if left to its own devices, your computer will slow down, sliding down the scale from the perfect end to the lousy end. When I comment on the slow system performance of a computer that just completed a 15-minute boot and logon, I am often surprised, or absolutely floored, when the owner says that it is acceptable. Although some people find “acceptable” to be, well, acceptable, as the saying goes, “good enough” is never good enough. As a CompTIA A+ Certified Professional, you should be able to identify areas that might cause slow system performance — and then resolve those issues.

In this chapter, you look at the major problems responsible for many slowdowns — and how to avoid them.

## *Identifying Areas of System Bottlenecks*

The tapered neck of a bottle, with its substantially smaller diameter than the body of the bottle, restricts the flow of liquid from the bottle.

Bottlenecks occur on your computer as well. They happen when most system resources are fine, except for that one subsystem that is heavily overused. To perform any task, a limited number of resources can be applied to a task; when the task exceeds the available resources, you run into problems. Computers have four critical resources that can be the source of a bottleneck:

- » Processor
- » Memory
- » Disk
- » Network



**FOR THE  
EXAM**

All system bottlenecks will occur in one of these four resources, which are the main subsystems in a computer.

In addition to resource overuse, hardware errors might also cause problems. This chapter does not examine possible hardware errors that can cause problems or issues that might be specific to a particular type of application or service. Most hardware issues are dealt with in Book 4, [Chapter 2](#), which is devoted to troubleshooting.

## *Using Monitoring Tools*

To effectively diagnose a problem in one of the four critical resources (processor, memory, disk, and network), you need to monitor what is going on with your system. In the following sections, you look at two tools that you can use to diagnose problems in these resource areas.

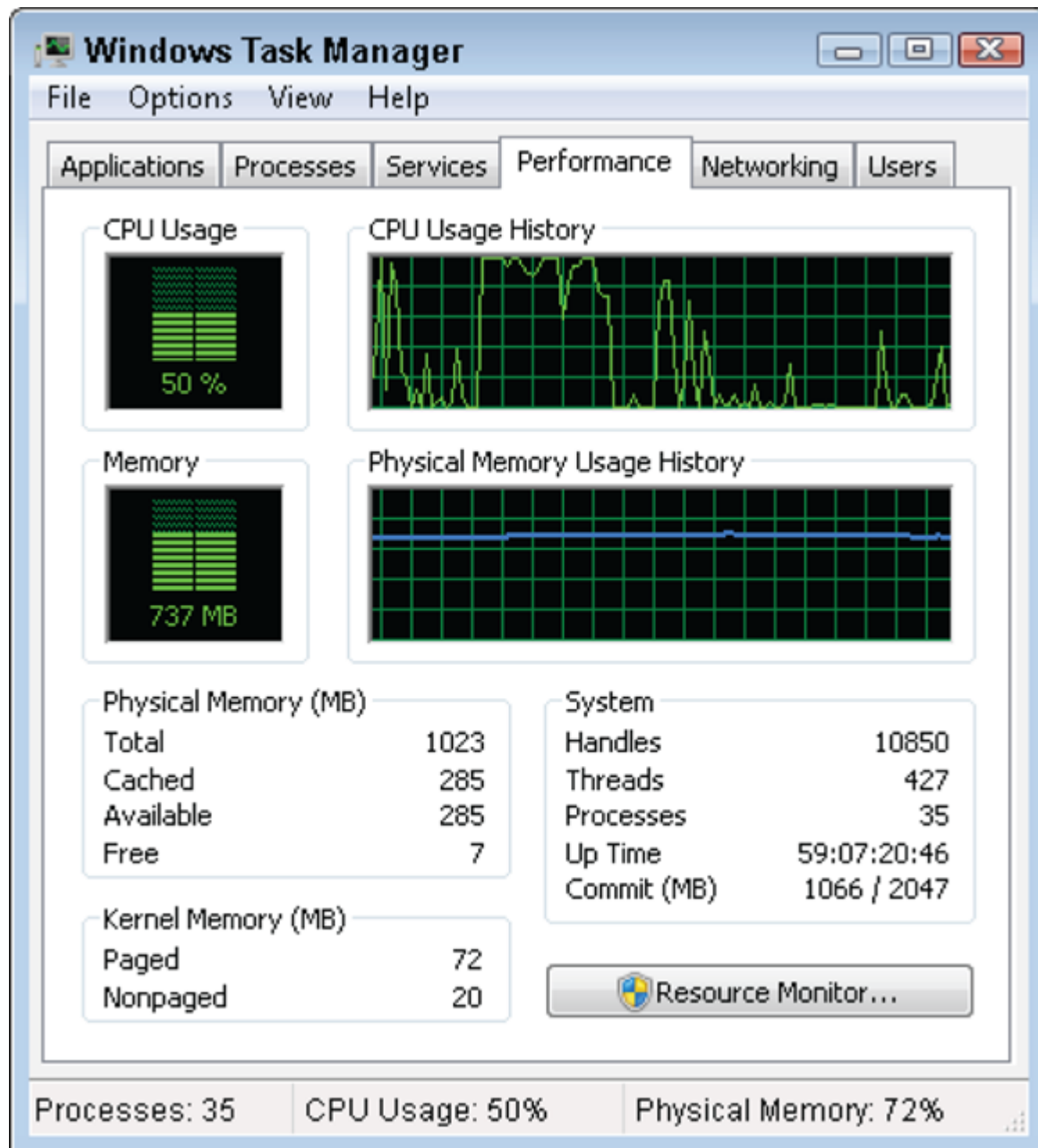
## ***Task Manager***

Task Manager (or `taskmgr.exe`) is a nice, quick, and simple tool. It is not as full-featured as Performance Monitor (see the following section), but what it lacks in features, it makes up for in simplicity and speed. To open Task Manager, press Ctrl+Alt+Del, which will display a list of options, of which Start Task Manager or Task Manager is one. You can also open Task Manager by right-clicking an empty area of the Taskbar and choosing Task Manager from the contextual menu.

## ***Performance tab***

You can use Task Manager to diagnose processor, memory, network, and service bottlenecks. [Figure 3-1](#) shows the Performance tab of Task Manager, which is typically the tab you will use first to identify a problem.





**FIGURE 3-1:** The Performance tab of Task Manager is usually the first place to look for problems.

On the Performance tab, you can find critical data about your system's performance. This tab is broken down into two main sections: the graphs and the numeric data. In the graph section is CPU usage and PF (Page File) usage information (or Physical Memory usage in Windows 7). In the numeric section, you see information on processes and memory usage. At

the very bottom of the window, you see summary information in the status bar.



**TIP**

The Task Manager window stays on top of all others, which is normally preferred; however, if you want it to go to the background, choose Options ⇒ Always on Top to deselect this option.

In the graphs section is the graph for the overall CPU usage, which is the same image shown in the system tray next to the clock. (This image appears automatically when you open Task Manager.) In this context, *CPU usage* is the average of CPU usage over all processors in your computer.

Next to this graph is a line graph showing you historic CPU usage over the past few minutes. If you have multiple processors, processors with hyperthreading, or multicore processors, you will see multiple line graphs, each in its own small window. If the graph is too small, resize Task Manager. And if you have multiple graphs, you can get a single graph showing the averages by choosing View ⇒ CPU History ⇒ One Graph, All CPUs. If you choose View ⇒ Show Kernel Times, you get a red line showing kernel processor utilization to help identify whether the problem is related to kernel processes or user processes. It is not uncommon for processor utilization to jump to 100 percent, but if it is consistently higher than 80 percent or 90 percent, you are likely experiencing a slowdown.

Page file usage (also recorded in the graphs section) is actually application-specific virtual memory usage, which includes paging file usage and a portion of the physical memory that the application is using. Just like CPU utilization, two graphs are shown here: a histogram for instantaneous usage and a line graph showing the historical usage. If you are running low on space in your page file, you are likely running short on memory. Windows 7 shows page file usage in the System section of the dialog, and shows physical memory usage in the graph area.

In the numeric section are totals for handles, threads, and processes. Think of *processes* as applications. However, not all applications run in

windows that you can see. Some, like services, run in the background, and these are included in the total number of running processes. Each process is composed of threads of code that are executed. Old applications from the 16-bit Windows and MS-DOS days are *single threaded*, which means that the program runs a single thread of code from beginning to end. Newer multithreaded applications can run several different threads of code, each performing a different task, all working together to perform the task that the processor is attempting to accomplish. On a multiprocessor computer, these threads can execute simultaneously, improving the overall speed of the process.

*Handles* are resources that the processes are using, such as memory locations, files, or Registry keys. Most likely, you will be primarily concerned with how many processes are running, because each running process consumes some of the total processor cycles available.

The other numeric sections all deal with memory — physical memory, kernel memory, and commit charge (prior to Windows 7). *Physical memory* is the actual RAM that is installed in your computer. In the physical memory section, you can see how much physical memory is on your computer, is free (or available), and is allocated to system cache or disk caching for the disk drives. The cache space dynamically adjusts as demands for memory go up, but the goal is to improve disk access by caching in fast memory.

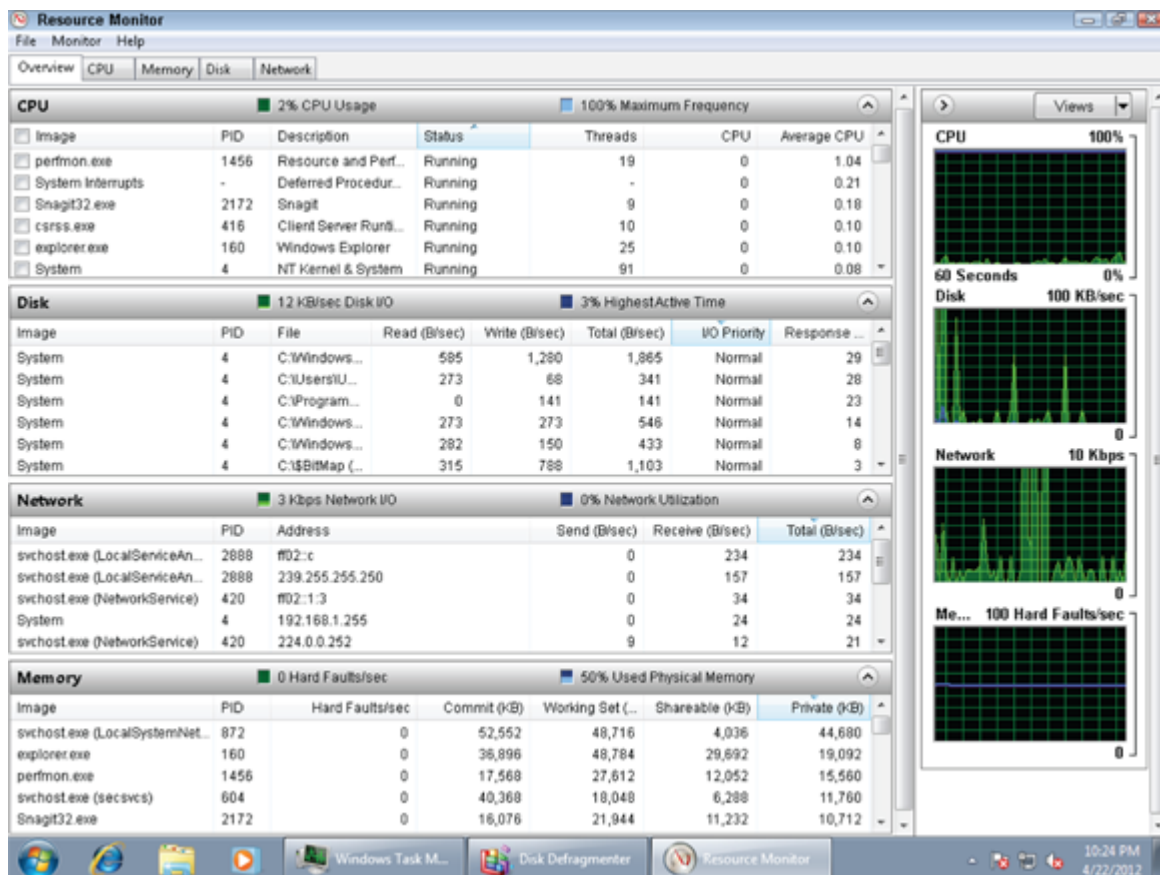
*Kernel memory* is memory allotted to the kernel. The kernel memory section shows you how much memory is allocated to the kernel, which is in charge of running all operations in your computer. If a driver has a memory leak, you might see kernel memory increase higher than normal for your computer, which is typically less than 100MB. The short-term solution is to reboot your computer.

Kernel memory is split between paged and nonpaged memory. Paged memory is part of the *page pool*, which is the memory swapped between physical RAM and the page file on the hard drive.

*Commit* is the amount of memory that is in use, or committed. This section shows you current usage, total available (including the page file), and the

peak usage since the last reboot.

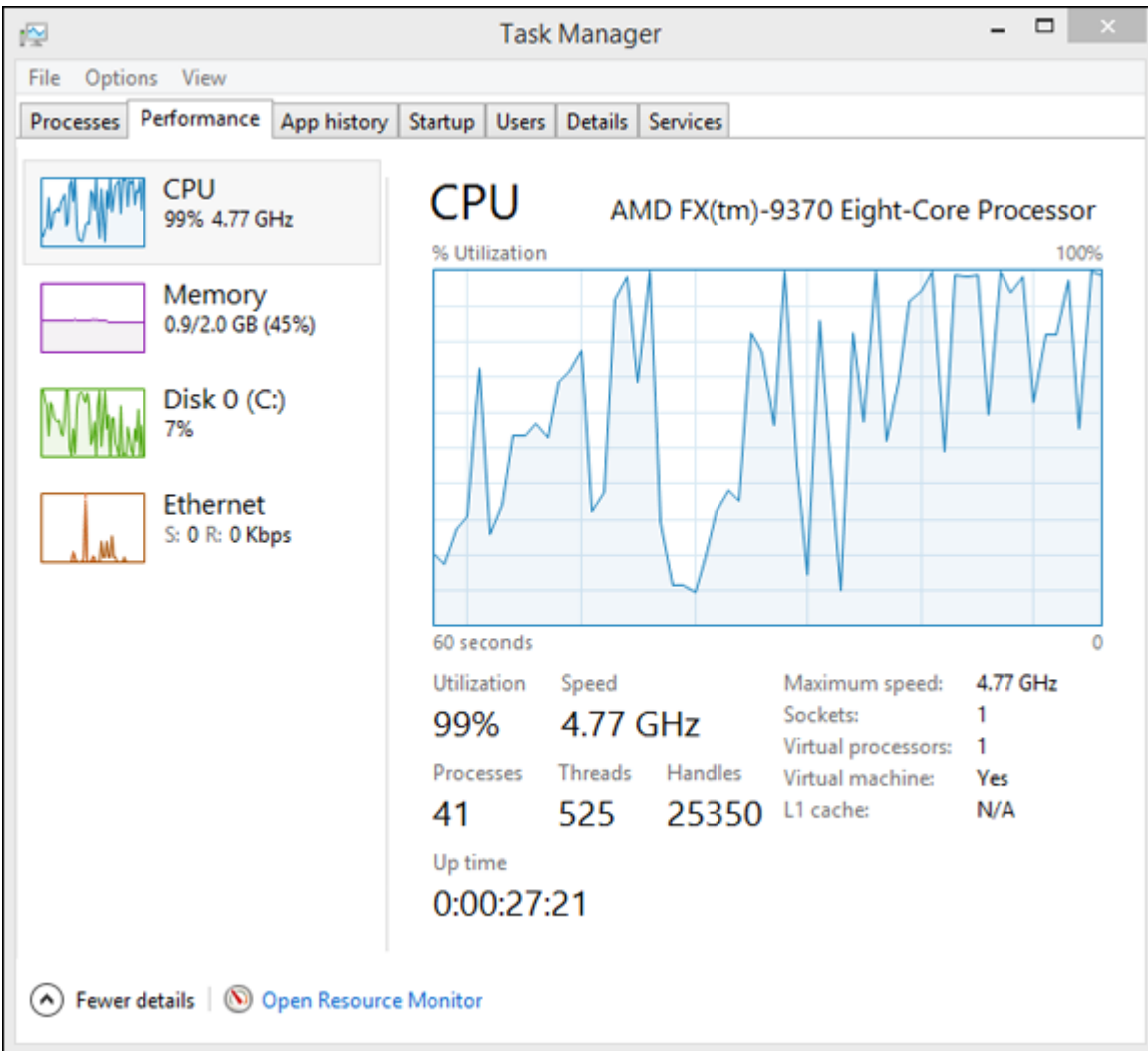
Windows has a Resource Monitor button to this tab, which opens another performance tool that provides more detailed information related to the four critical resources, as shown in [Figure 3-2](#). One big difference between Resource Monitor and Task Manager is that Resource Monitor shows the resource usage by application or process. Resource Monitor is covered in the section “[Windows Resource Monitor](#),” later in this chapter.



**FIGURE 3-2:** Resource Monitor shows detailed information related to processes.

Windows 8.1 and Windows 10 completely rework the Performance tab of Task Manager by providing a series of graphs and numeric data similar to what you would see in Resource Monitor, but substantially scaled back. This new interface, shown in [Figure 3-3](#), can be seen by opening Task Manager and clicking on the More Details link. Key points of the new interface include:

- » Summary graphs on the left side of the window show highlights of all four critical resources.
- » CPU graphs include key processor data such as processes, threads, and handles.
- » CPU graphs have the option of showing one graph per CPU, as well as showing kernel time. These options are accessed by right-clicking the graph.
- » Memory graphs show table data for available, committed, changed, and in-use memory.
- » Disk graphs show disk busy and idle time, transfer rates, whether the drive has a page file, and formatted capacity.
- » Network (Ethernet) graphs show transfer rates, whether the network interface is active, and some configuration information.



**FIGURE 3-3:** Windows 8.1 enhances the information displayed on the Performance tab.

As with earlier versions of Windows, the Performance tab includes a link to the Resource Monitor, which allows a more detailed analysis of system performance.

### *Networking tab*

In most cases, looking at the data on the Performance tab leads you to either the Processes tab or the Networking tab (on Windows 7). On the Networking tab is a line graph with lines for each network interface on your computer, representing the percentage of bandwidth being used by each one. To see additional information on your graph, choose an option from the View ⇒ Network Adapter History submenu. This allows you to add Bytes Sent and Bytes Received to the existing Bytes Total line on the

graph. This is useful for seeing whether a network-related problem is because of data coming in or going out.

You can also find the same information from the graph presented numerically at the bottom of the window. To see more data, choose View ⇒ Select Columns. This opens the tool to a lot more troubleshooting capabilities by allowing analysis of many network-related counters, such as the breakdown of bytes sent, bytes received, and traffic type being unicast or nonunicast. *Unicast* network traffic is information that is sent only to your computer; *nonunicast* traffic is simultaneously sent to multiple computers on your network.

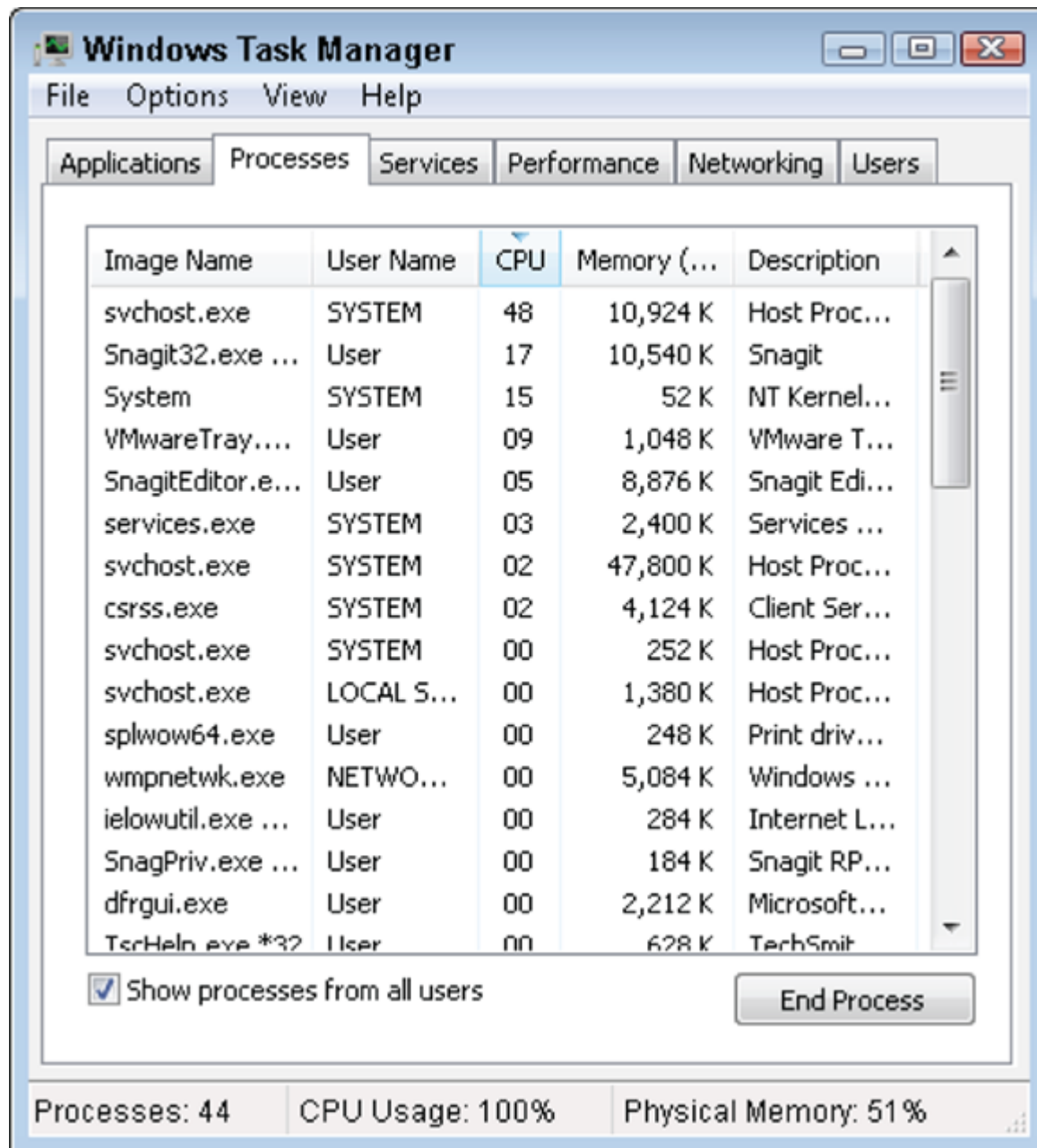


**TIP**

When working with Windows 8.1 or Windows 10, networking data is seen on the Performance tab, eliminating the need for a Networking tab. Detail data about bytes transferred and throughput can be seen by right-clicking the network graph and selecting View Network Details.

### ***Processes tab***

If the problems are not network-related, you might be led to look at the Processes tab, which is shown in [Figure 3-4](#) for a Windows 7 computer. This tab lists all running processes on your system in columns. You can toggle a sort on the columns (ascending or descending) by clicking the column heading. The default columns include Image Name, User Name (the user executing the process), CPU (the percentage utilization of this process), and Memory (the amount of memory this process is using). If you are logged on as an administrator, you can also choose to Show Processes from All Users to see processes other than your own. For Windows 8.1 and Windows 10 users, the Processes tab shows a summary of the objects found on the Performance tab, while the Details tab shows information equivalent to the Windows 7 Processes tab.



**FIGURE 3-4:** The Processes tab of Task Manager helps identify CPU utilization problems.

In most cases, you will be able to locate the process using up most of the CPU cycles and slowing down your computer. To see additional troubleshooting information, choose View ⇒ Select Columns to select from many other counters, such as Virtual Memory Size, Page Faults, and Peak Memory Usage, to list just a few.



*Page faults* occur when information that your computer wants is not in physical memory and must be initially loaded into memory or be read from the page file on the hard drive. If the number of page faults takes a sharp rise, you might also notice that your available memory is low.



**TIP**

Right-clicking any running task on the Processes tab invokes a contextual menu with several options, including ending the process, ending the process tree, going to the service, and changing the application priority or the processor affinity (if you have more than one processor). If you end the process tree, you terminate the process and any other processes that it started. If you have right-clicked on a process which is used by a service on your computer, then selecting Go to Service(s), will bring you to the Services tab where all related services will be automatically selected. Changing a process's priority changes the percentage of CPU time that an application gets when it is running. If you set the affinity, then you are able to force it to run on a specific processor.



**WARNING**

Be careful when using high and real-time priorities; they can cause system instability. If you have a highly active program, such as a counter, setting it to real-time priority can allow it access to all CPU cycles on your computer, which can cause the system to ignore user input from the mouse or keyboard, preventing you from doing anything else with your computer.

The additional options available in the contextual menu include:

- » **Analyze wait chain (Windows 8.1 and Windows 10):** Displays the process tree and identifies which processes in the tree are causing a wait state for other processes. Processes in the tree may be terminated at any position in the tree.

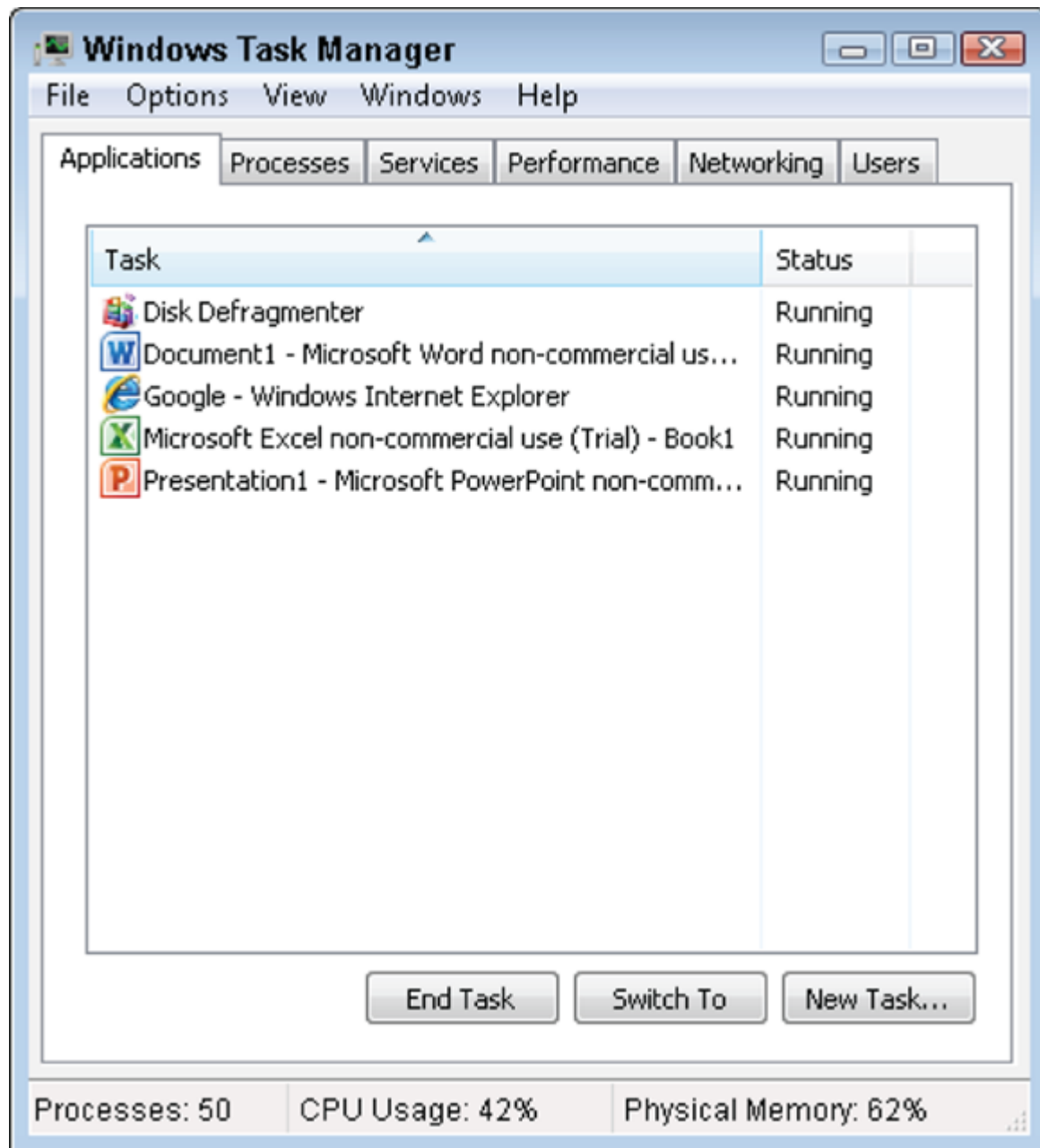
- » **Create dump file:** Creates a memory dump file for troubleshooting. This is the same file that is created when an application crashes, but this option enables you to create these files on demand.
- » **Open file location:** Opens the folder containing the executable or process image.
- » **UAC Virtualization:** Allows you to enable UAC Virtualization, which enables process to be written to a user profile location, allowing non-administrative users to save these settings under their own accounts. Effectively this allows non-administrative users to install applications under their own account.

### *Services tab*

The Services tab shows you the same list of services that you will find in the Services MMC management tool, but in an abridged format. This allows you to stop or start these services, or launch the Services MMC to have full control of the services. When you right-click a service, you have the option of going to the process, for services that have processes listed on the Processes tab. This makes the job of troubleshooting runaway processes and services much easier.

### *Applications tab*

The Applications tab shows what applications are running in the foreground (as shown in [Figure 3-5](#)). These applications should list Running in the Status column. If the application is not listed as running, it may not be responding. At this point, you can either give the application more time to respond (after all, it might just be busy), or you can end a task by selecting the application and clicking the End Task button. To bring an application's window to the foreground, select the application and click the Switch To button. If you want to locate the application on the Processes tab, right-click the application and choose Go to Process. To launch a new application, click the New Task button, which brings up the Run dialog box.



**FIGURE 3-5:** The Applications tab lists running foreground applications and their responsiveness.

### *Users tab*

The Users tab shows which users are logged on, if they are currently active, the remote computer they are connected from (Client Name), and the session they are logged on to (either remote or console). For any of the users who are connected, you are able to disconnect the user or to log the user off.

On Windows 8.1 or Windows 10 computers, you are able to use this tab to show utilization per user, expand the user to see the applications he is using, access the user's control panel, and disconnect the user.

### *Startup tab*

New with Windows 8, the Startup tab shows a list of applications that are set to start automatically with the OS or when a user logs on. From this tab you are able to disable the auto-start of the application.

## *Performance Monitor*

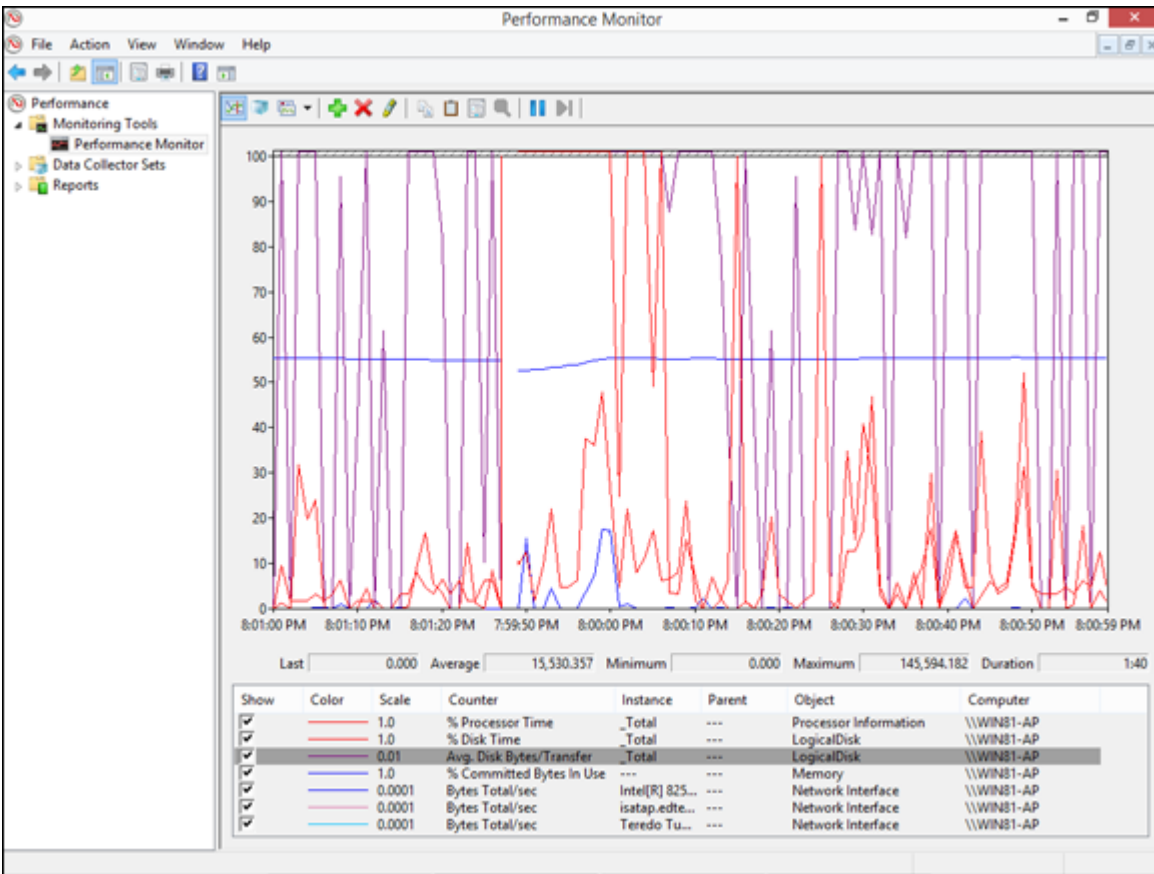
Although Task Manager might be where you first look for solutions to performance problems, it is really a 10,000-foot view of the situation. To get down to ground level, you need a more powerful tool, and that is where the Performance administrative tool comes in, with its two main components: Performance Monitor and Data Collector Sets.



**TIP**

Windows 7 has gone back to the Performance Monitor name and still provides reliability information in the form of the Reliability Monitor. To open the Reliability Monitor, choose Start ⇒ Control Panel ⇒ System and Security ⇒ Action Center ⇒ Maintenance ⇒ View Reliability History.

Performance Monitor is Task Manager's big brother. It does not allow you to change settings or terminate tasks, but it does allow you to monitor a whole series of available counters. Launch Performance by choosing Start ⇒ Control Panel ⇒ System and Security ⇒ Administrative Tools ⇒ Performance Monitor, or by running either `perfmon.exe` or `perfmon.msc`. A counter is a numeric measure of an element of a system component, such as bytes of available memory. [Figure 3-6](#) shows the standard graph display for a custom set of counters. The only default counter is % Processor Time from the Processor object which shows processor utilization problems.



**FIGURE 3-6:** Performance Monitor shows graphs for a variety of counters built into Windows.



**FOR THE  
EXAM**

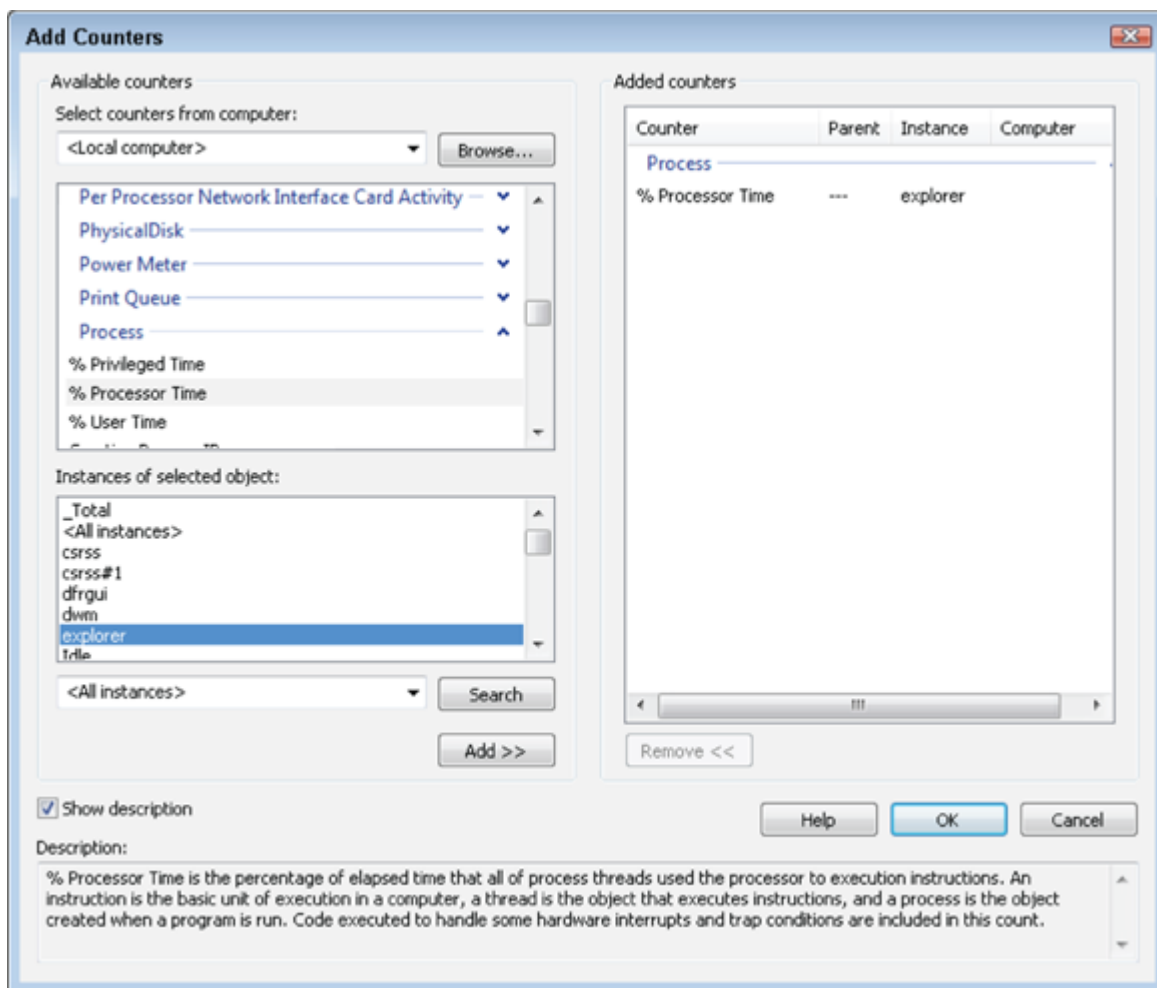
On the A+ exams, you might see references to System Monitor as well as Performance or Performance Monitor. *System Monitor* was the component of Performance that makes the graphs of current and logged activity. Current Windows OSes have gone back to calling the component that makes the graphs *Performance Monitor*.

For each counter, you will see a graph with 100 readings, which by default are taken once per second. To change this frequency, bring up the Properties for the graph by clicking the Properties button on the toolbar or by pressing Ctrl+Q and changing the value of Sample Automatically Every X Seconds. You will have to select the General tab of the Performance Monitor Properties dialog, and in addition to changing the

sample frequency, you will also be able to change how many samples will fill the graph.

If you don't like the line graph look, click the View Histogram button (think bar graph) or View Report button (gives only numeric data). These buttons are indicated in [Figure 3-6](#).

Many other counters can be added to the graph. If you click the Add button on the toolbar or press Ctrl+I, you can add counters to your graph, as shown in [Figure 3-7](#).



**FIGURE 3-7:** A wide variety of counters may be added to your graph.

By default, you add counters from *your* computer, but you have the option to add counters for any computer that you have admin rights for. If you prefer to view counters from a remote computer, choose it from the Select

Counters from the Computer drop-down menu to type the computer name into the drop-down menu box. If you choose another computer, your list of Performance objects is updated to include the objects on that computer. Many counters are defaults for the OS, and any software you install has the option of adding custom counter objects, which is the case for many Microsoft programs. If you look at the list of counters, you will see that they can be categorized into the four critical system resources: processor, memory, disk, and network. [Table 3-1](#) lists some of the related objects for the four critical system resources.

**[TABLE 3-1](#) Related Objects for Critical System Resources**

<i>Critical System Resource</i>	<i>Related Object</i>
Processor	Process
	Processor
	System
Memory	Memory
	Paging File
Disk	Cache
	Physical Disk
Network	Browser
	IP
	Network Interface
	Redirector
	Server
	Server Work Queues

[Table 3-1](#) is just a partial list of all the possible objects available to you. Each object has a series of related counters. For instance, the Process object has counters for % Privileged Time, % Processor Time, and % User Time. Each counter may have a series of *instances*. In the case of the Process object and % Processor Time, there are instances for each running process on the system.



**TIP**

For any counters that you do not know, select that counter and then select the Show Description check box to access a description about that counter.

When you click the Add button to add a counter to your graph, the new counter lines show up immediately. When you have added all the counters you want to view, click Close or OK.



**TIP**

When you have many lines on your graph, click the Highlight button or press Ctrl+H to highlight the line in bold on your graph for any counter you selected on the bottom part of the screen. To delete any counters that you added, select the counter and click the Delete button on the toolbar or press the Delete key on your keyboard.

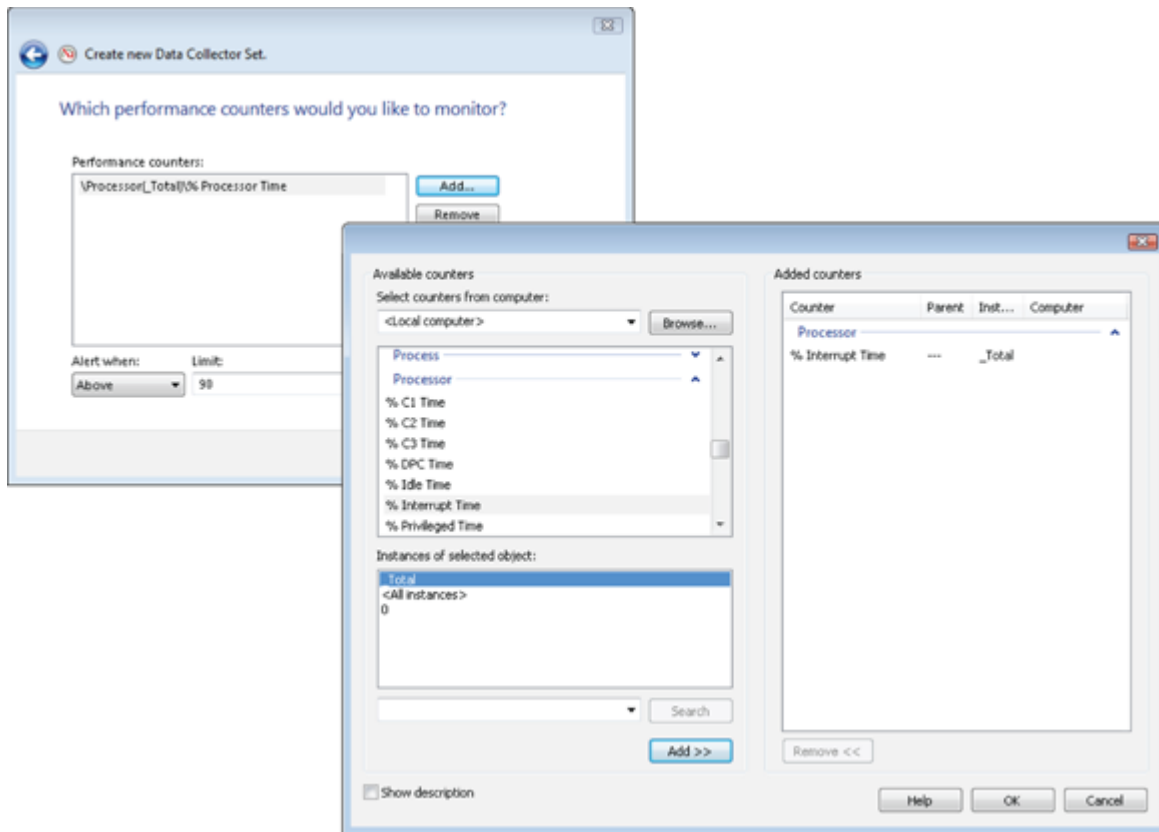
So far, you have been taking data from current activity. If the problem is periodic, you want to create logs and alerts to try to catch the problem when it occurs. If you want to create an alert based on your counters, this is done with Data Collector Sets. To create an alert, follow these steps:

1. **Expand Data Collector Sets in the navigation pane and then right-click User Defined, and choose New ⇒ Data Collector Set.**
2. **In the Create New Data Collector Set dialog, you provide a descriptive name used to identify the alert, choose the Create Manually radio button, and click the Next button.**
3. **Choose the Performance Counter Alert and click the Next button.**  
On this screen, you will then be able to use the Add button to select counters and set the alert-firing threshold for each counter, as shown in [Figure 3-8](#).
4. **After adding your counters, click OK and set the threshold value for each counter.**
5. **To finish off the alert, click Next.**



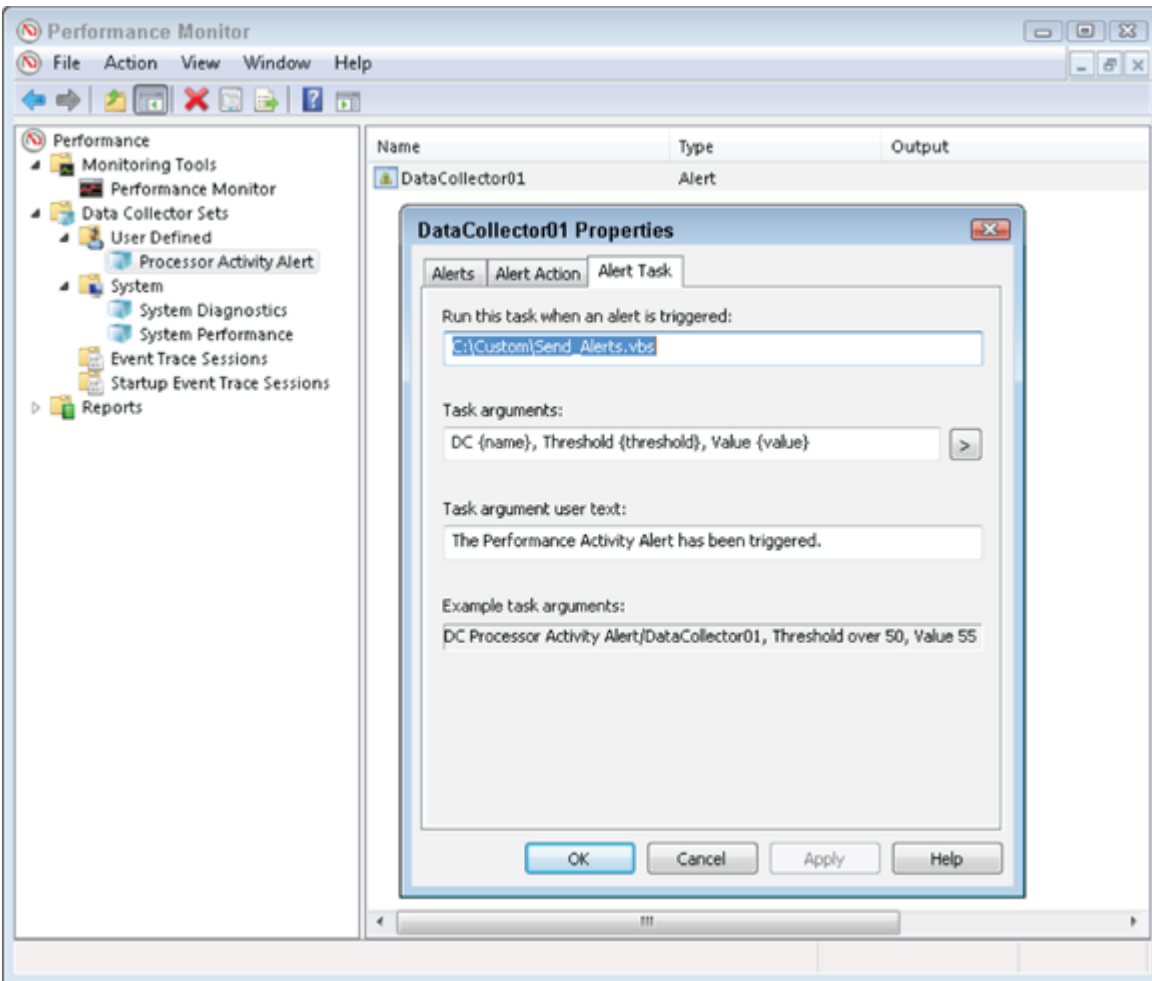
The last portion of the wizard brings you to a screen to set the credentials to be used to run the alert (which affects what actions may be performed), as well as the option of saving and starting the data collector right away or editing the settings.

**6. Click Finish to complete the process.**



**FIGURE 3-8:** Add counters and set alert thresholds.

To complete the alert configuration, you will need to open the data collector properties and adjust the settings. From within the User Defined Data Collector Sets, select a Data Collector Set that shows the contents of the set in the right pane, with the default name being `DataCollector01` for the first data collector. Right-click the data collector and choose Properties. This allows you to adjust the performance counter thresholds on the Alerts tab, write to the application log and start a Data Collector Set on the Alert Action tab, or specify actions to be performed on the Alert Task tab, as shown in [Figure 3-9](#).



**FIGURE 3-9:** Set alerts to notify you of problem conditions.

These values are checked at the Sample interval. When the firing threshold criteria are met, the actions on the Alert Action and Alert Task tabs are performed. The alert action will be a custom executable or script that allows you to perform additional actions. The alert will be active during the times listed on the Schedule tab of the Data Collector Set's properties.

Rather than looking at the current activity, you can also create a log of counter activity that may be reviewed at a later date. Just like the alerts, you can choose a schedule for this log so that it can run at a specific time. For instance, if you are having problems with a computer regularly between 2 p.m. and 4 p.m., you could schedule the log to run from 1 p.m. to 5 p.m. You can also have the log file stop when the file is full or reaches its configured maximum size. When the logging stops, you can

have a program run, which might be used to notify you that the logging has stopped or to copy your new logs to another computer or location.

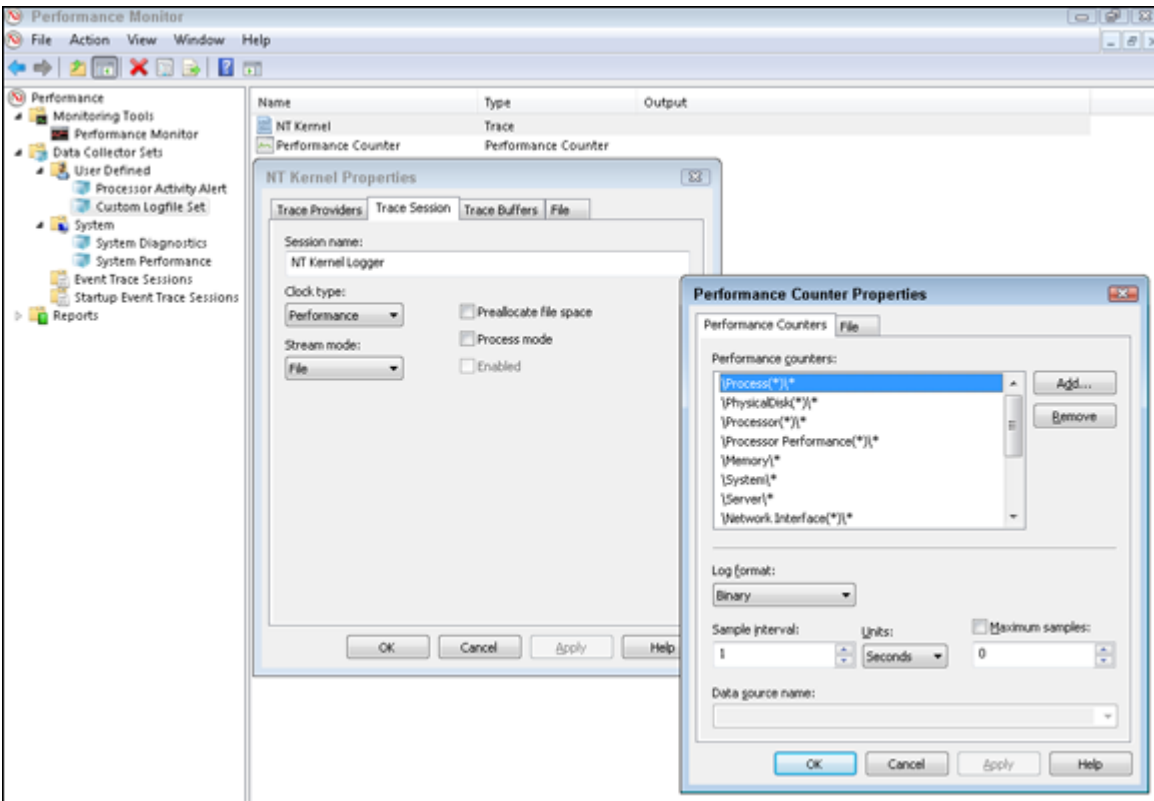
To create a log, you will again use the Data Collector Sets. To create a log, follow these steps:

1. **Expand Data Collector Sets in the navigation pane, and then right-click User Defined, and choose New ⇒ Data Collector Set.**
2. **In the Create New Data Collector Set dialog, you first provide a descriptive name used to identify the alert, choose the Create from a Template radio button, and then click the Next button.**
3. **Choose the System Performance template and click the Next button.**
4. **Use the default root directory to store the logs for this Data Collection Set or specify your own directory, and click Next to continue.**

The last portion of the wizard brings you to a screen to set the credentials to be used to run the alert (which affects what actions may be performed), as well as the option of saving and starting the data collector right away or editing the settings.

5. **Click Finish to complete the process.**

[Figure 3-10](#) shows the two types of data collection processes that are running. One tracks kernel performance stats, while you will be more interested in performance counter properties. If you did not start the log file collection at the end of the creation process, you can right-click the Data Collection Set and choose Start to start collecting log data. You can change how long the log files will collect by editing the settings on the Stop Condition tab of the Data Collection Set properties.



**FIGURE 3-10:** Performance counter logs can be used to record data for historical analysis.

After a log file is created, you can view it from the Performance Monitor by clicking the View Log Data button or by pressing Ctrl+L. You are asked for the name of the log file that you want to use, and then you can add counters to the graph normally, but you can choose only from the counters included in the log file. The resulting graph charts all readings taken for the counters, not just the default 100 readings. The default log file location is the %systemdrive%\PerfLogs\Admin directory.

To change the time range displayed on the graph, click the Properties button and the Source tab, from which you can adjust the time range. As you adjust the range, a vertical bar moves through the graph, showing you where that range is. To return to getting graph data from current activity, click the View Current Activity button or press Ctrl+T.

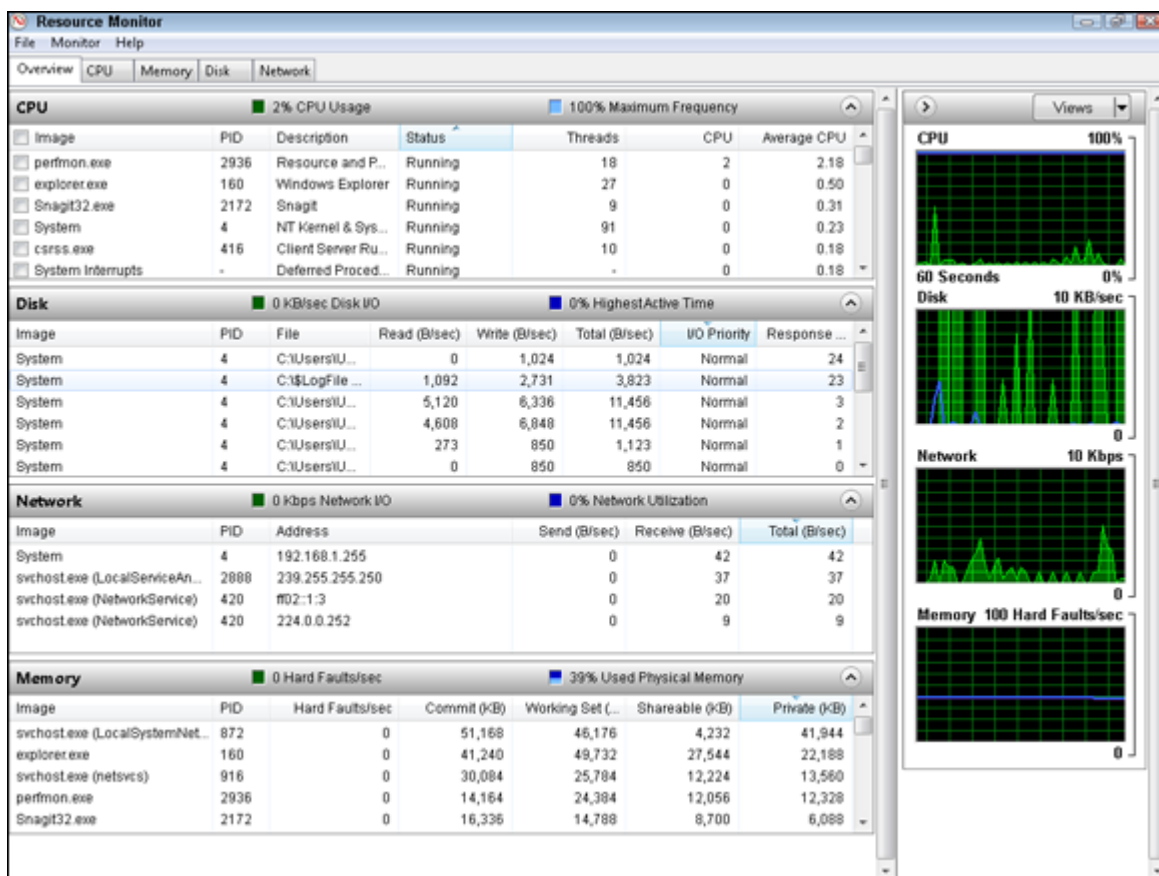
## ***Windows Resource Monitor***

Whereas Task Manager is a simple tool that easily shows you key performance statistics at a glance, and Performance Monitor is a powerful, complex, customizable tool for delving into detailed

information about system performance, Windows Resource Monitor strikes a middle ground. It was introduced before Windows 7 and has been enhanced in newer version of Windows.

## Overview

An easy way to open Windows Resource Monitor is to click the link on the Resource Monitor button on the Performance tab of Task Manager. On the initial window, shown in [Figure 3-11](#), Resource Monitor will show you key summary information across all four resource categories: CPU, disk, network, and memory. If you see issues with your system related to performance, this initial screen should offer suggestions as to which of the four critical resources are being overconsumed.



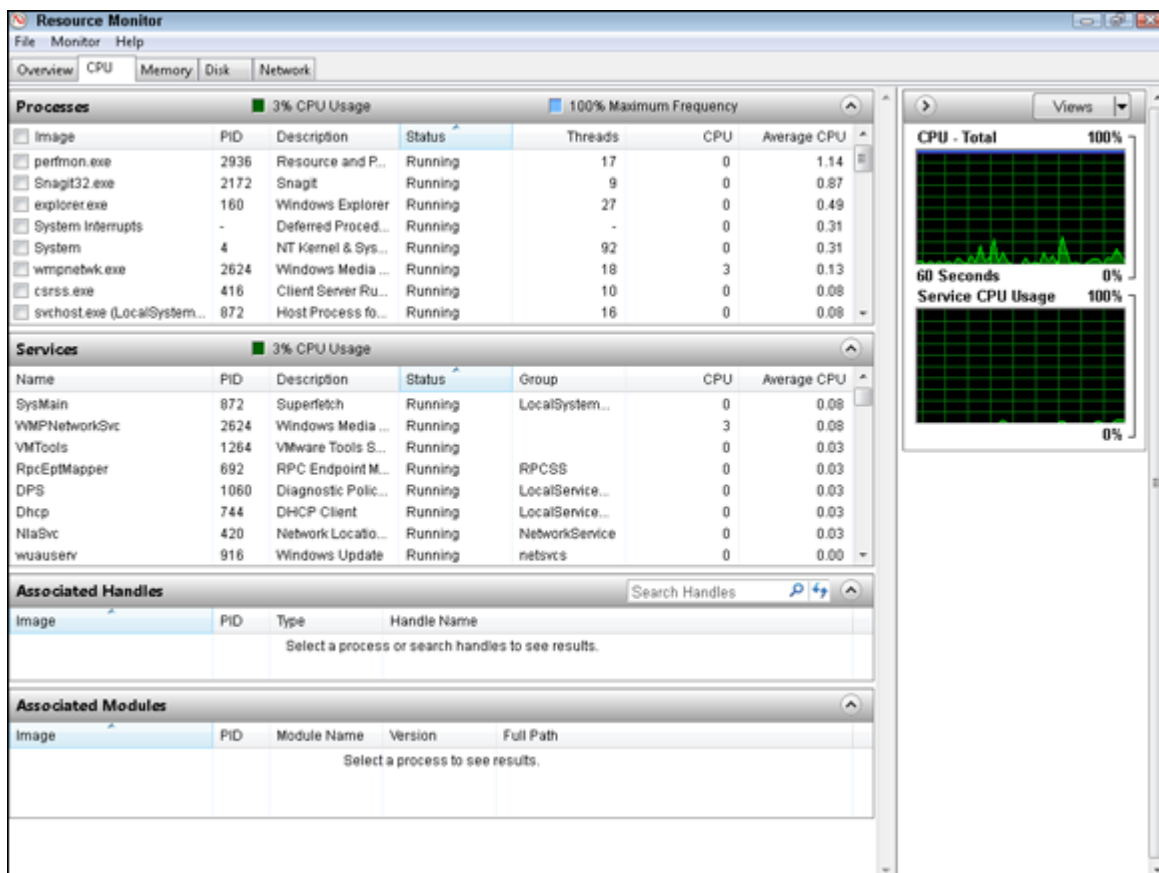
**FIGURE 3-11:** Resource Monitor will show data regarding all four resource categories.

Each table of data in Resource Monitor allows you to add or remove columns from the display, providing you with additional detail.

To view additional information related to each of the resource categories, you can choose the appropriate tab at the top of the application window.

## CPU

The CPU tab provides detailed information related to processes that are consuming processor cycles on your computer. Issues in the CPU area will show up as highly busy threads in the processes or services categories. In addition to the tables of performance data, you also find two charts showing CPU utilization, as can be seen in [Figure 3-12](#).



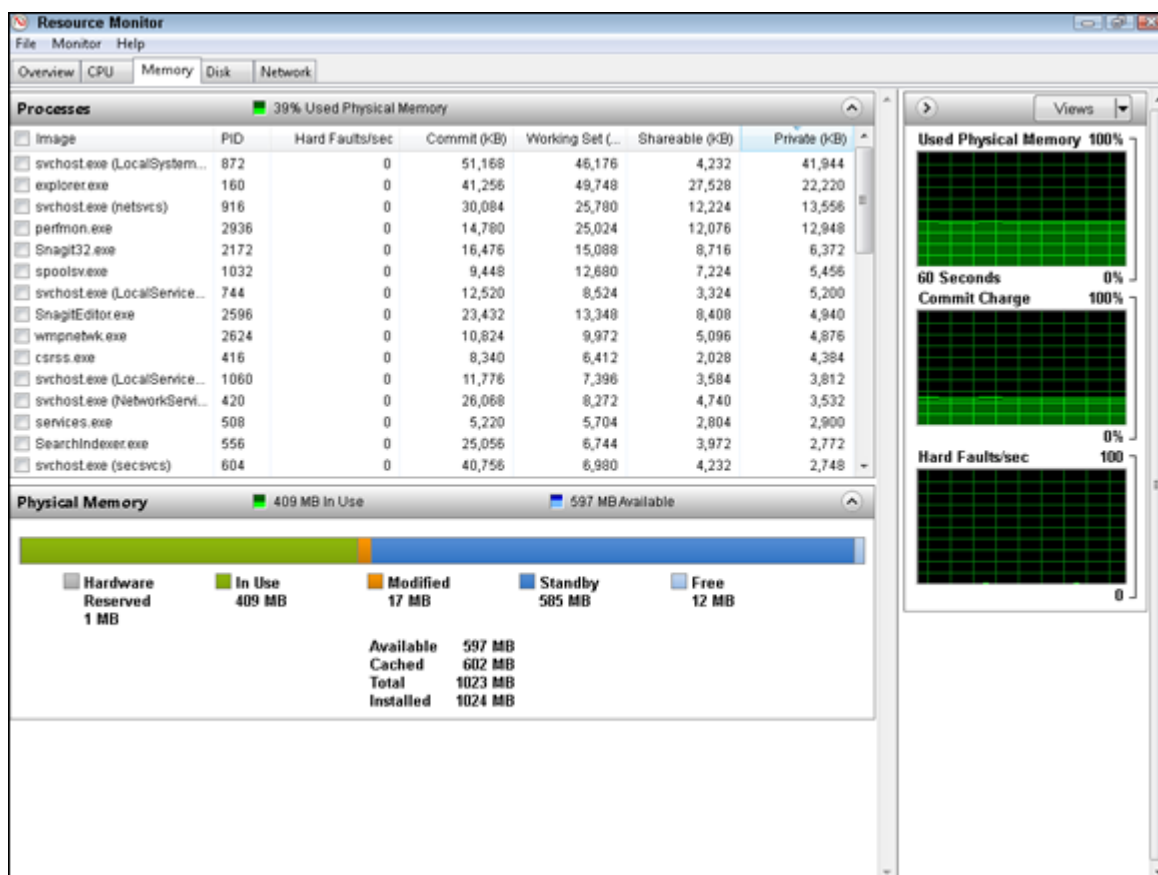
**FIGURE 3-12:** CPU data will identify issues with processes or applications that are overutilizing the CPU.

While troubleshooting issues with processes, you can right-click a process and choose End Process or End Process Tree, as you can with Task Manager. In addition to these options, you can choose Suspend Process and Resume Process (temporarily pausing the process rather than stopping it) and Analyze Wait Chain. If you use Analyze Wait Chain for a

process, you will be able to see whether issues with this process are actually a result of other processes that are waiting for processes to be completed.

## Memory

If you find that the performance issues are related to memory, the Memory tab is where you should focus your attention. [Figure 3-13](#) shows that this again gives you a table of processes, but this time, it shows you memory statistics related to each process in addition to a chart showing you how that memory is allocated.

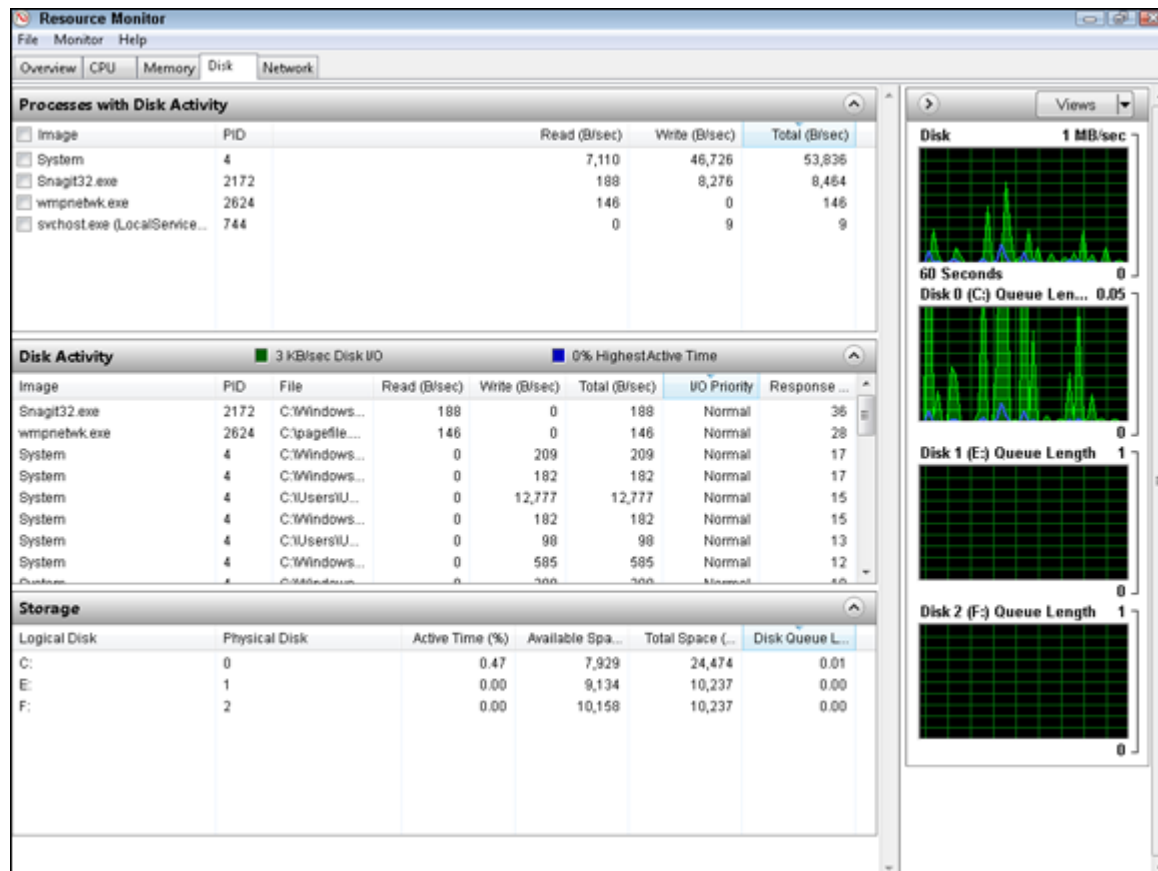


**FIGURE 3-13:** Memory statistics will identify memory consumption issues.

Memory-related performance issues should be identifiable on this page, with a focus spent on the processes that are consuming the greatest amount of memory.

## Disk

Because not all processes make use of the hard drive, the Disk tab, as seen in [Figure 3-14](#), filters down the list of processes to only those that have disk activity. From this page, you can see the process, its disk activity, the files that are read or written to, and the overall disk utilization per disk. Higher-than-normal disk activity may be related to problems with the process, or it can identify processes that are overconsuming resources.



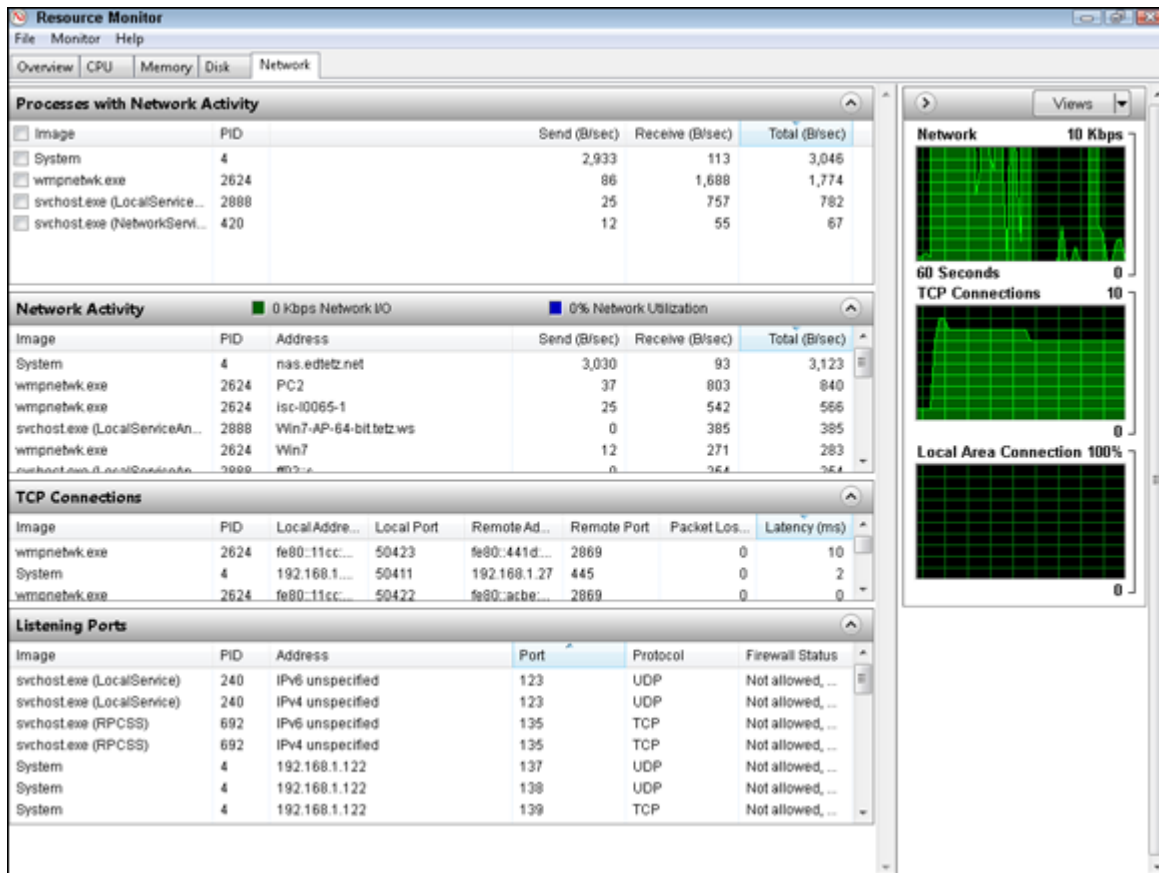
**FIGURE 3-14:** Disk activity identified by process.

## Network

Resource Monitor's Network tab, shown in [Figure 3-15](#), provides you with detailed data on network utilization. As with the disk, this tab will filter out processes that do not generate network traffic, and for remaining services, you will see the network traffic that is generated for each process. In addition to the network activity, you will see tables listing the



active TCP connections as well as any ports that are open to accept incoming connections.



**FIGURE 3-15:** Network activity can be viewed in great detail.

Network activity shows not only the data throughput through the network cards, but also the network addresses that are used by each of the processes.

## Other tools

Windows has introduced two tools in an attempt to allow for more functions to be completed from the command line interface:

`tasklist.exe` and `taskkill.exe`. These tools take the functionality of the Processes and Services tabs of the Task Manager and bring them to the command line. One additional feature of these programs is that they can be run locally on the computer, or they can be used to view processes on another computer on the network.

The `tasklist.exe` program will show you what processes are running on the computer, which can be seen in greater detail using the `/v` option, which is just one of many options. The basic output from the command looks like [Listing 3-1](#):

### **LISTING 3-1 tasklist.exe Output**

---

```
C:\Users\User>tasklist

Image Name PID Session Name Session# Mem Usage
=====
System Idle Process 0 Services 0 24 K
System 4 Services 0 2,312 K
smss.exe 416 Services 0 640 K
csrss.exe 504 Services 0 3,932 K
wininit.exe 540 Services 0 3,816 K
csrss.exe 560 Console 1 3,260 K
winlogon.exe 604 Console 1 4,736 K
ashDisp.exe 4044 RDP-Tcp#0 2 4,496 K
wmpnscfg.exe 4052 RDP-Tcp#0 2 5,004 K
svchost.exe 2180 Services 0 4,648 K
EasyCapture.EXE 2324 RDP-Tcp#0 2 7,404 K
mmc.exe 3692 RDP-Tcp#0 2 27,344 K
taskmgr.exe 3380 RDP-Tcp#0 2 9,548 K
cmd.exe 3528 RDP-Tcp#0 2 2,464 K
WmiPrvSE.exe 2216 Services 0 9,036 K
tasklist.exe 1892 RDP-Tcp#0 2 5,992 K
```

The `taskkill.exe` program is used to terminate tasks that you need to stop, in the same manner you would with End Process option in Task Manager. If I were to terminate the `EasyCapture.exe` process in [Listing 3-1](#), I would be able to run the following command:

```
taskkill /PID 2324
```

## ***Optimization Best Practices***

There are many simple steps that you can take to optimize your system for best performance. Some components that you can make changes to include virtual memory, hard drives, printers, scanners, system services, running processes, and temporary files. After you make changes to the

components, you can use Task Manager and System Monitor to see whether your changes had any effect on system performance.

## *Virtual memory*

*Virtual memory* uses both RAM and hard drive space to create a memory pool. The hard drive space used is called a paging file; in Windows, the filename is `pagefile.sys`. Access to the paging file is much slower than access to RAM, so the paging file is used for information that is accessed less often. The default paging file size is 1.5 times the amount of RAM in your computer. To improve performance, you should not set this any larger than it really needs to be. You can find out what your maximum size should be by running your system for several days of typical or hard use and then checking your peak usage in Task Manager or System Monitor. Set your paging file size between 1.25 times to 1.5 times your peak paging-file usage. To see how to gather your memory usage data using Task Manager or System Monitor, review the “[Using Monitoring Tools](#)” section earlier in this chapter; and to see how to change the size of your paging file, read Book 5, [Chapter 2](#).



**TIP** Windows now defaults to a page file setting of System Managed Size, which will initially set the page file to the amount of RAM on your system and then dynamically adjust the size as needed by the system. This takes away much of the effort in maintaining your page file.

If you find that you are using a lot of virtual memory and accessing the paging file, you need to either reduce the processes using RAM or add more RAM (see Book 2, [Chapter 3](#)) to improve overall system performance by reducing paging-file usage.

If neither step is an option, move the page file to a drive other than the drive that holds your Windows installation. You should also choose the fastest drive that you have. That is, solid state drives over hard disk drives, 7,200 rpm or 10,000 rpm drives over 5,400 rpm drives, ATA 133

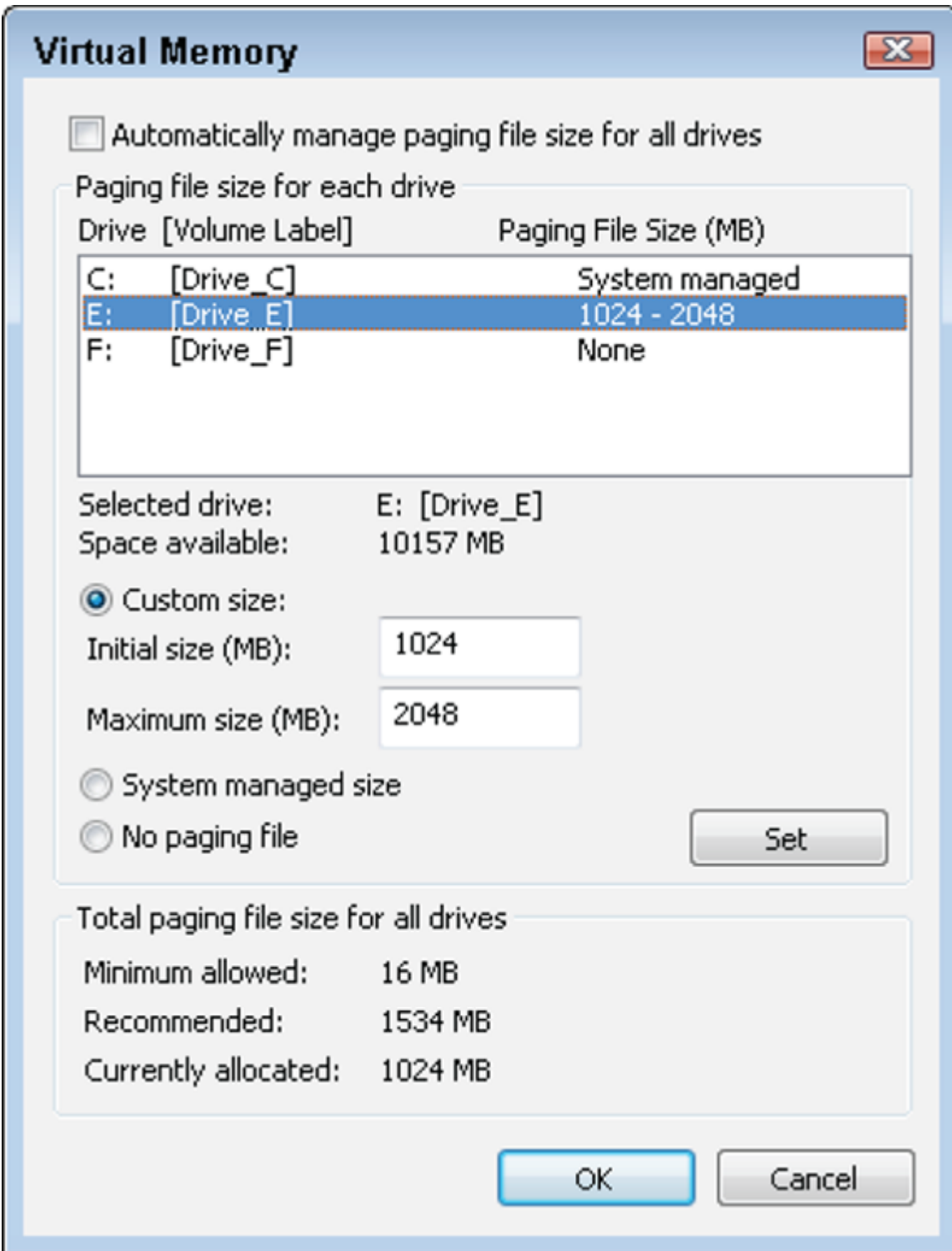
drives over ATA 66, and so on. The chosen drive should not have other highly intensive processes using it.



**TIP** To avoid having your page file fragmented, defragment your drive prior to creating your page file. Microsoft has a downloadable Sysinternals tool called PageDefrag, which will defragment your page file on reboots of your computer. PageDefrag and other Sysinternals tools can be downloaded from <http://technet.microsoft.com/en-us/sysinternals>.

To change the location of your paging file, follow these steps:

1. **Choose Start ⇒ Control Panel and open the System applet.**
  2. **Click the Advanced tab and click the Performance Settings button.**
  3. **In the Performance Options dialog box, click the Advanced tab and then click the Virtual Memory Change button.**
  4. **From the Virtual Memory dialog box, shown in [Figure 3-16](#), select the drive you want the paging file saved on, choose the size, and then click the Set button.**
  5. **To finish, press the series of OK buttons to close the dialog boxes.**
- Depending on the changes you made, you may need to reboot your computer.



**FIGURE 3-16:** Changing the page file settings can improve your overall system performance.

Depending on the Startup and Recovery setting in your System control panel applet, you might require a paging file on the drive that contains

your Windows directory that is at least equal to the amount of RAM installed in your computer.

## *Hard disk drive and solid state drive*

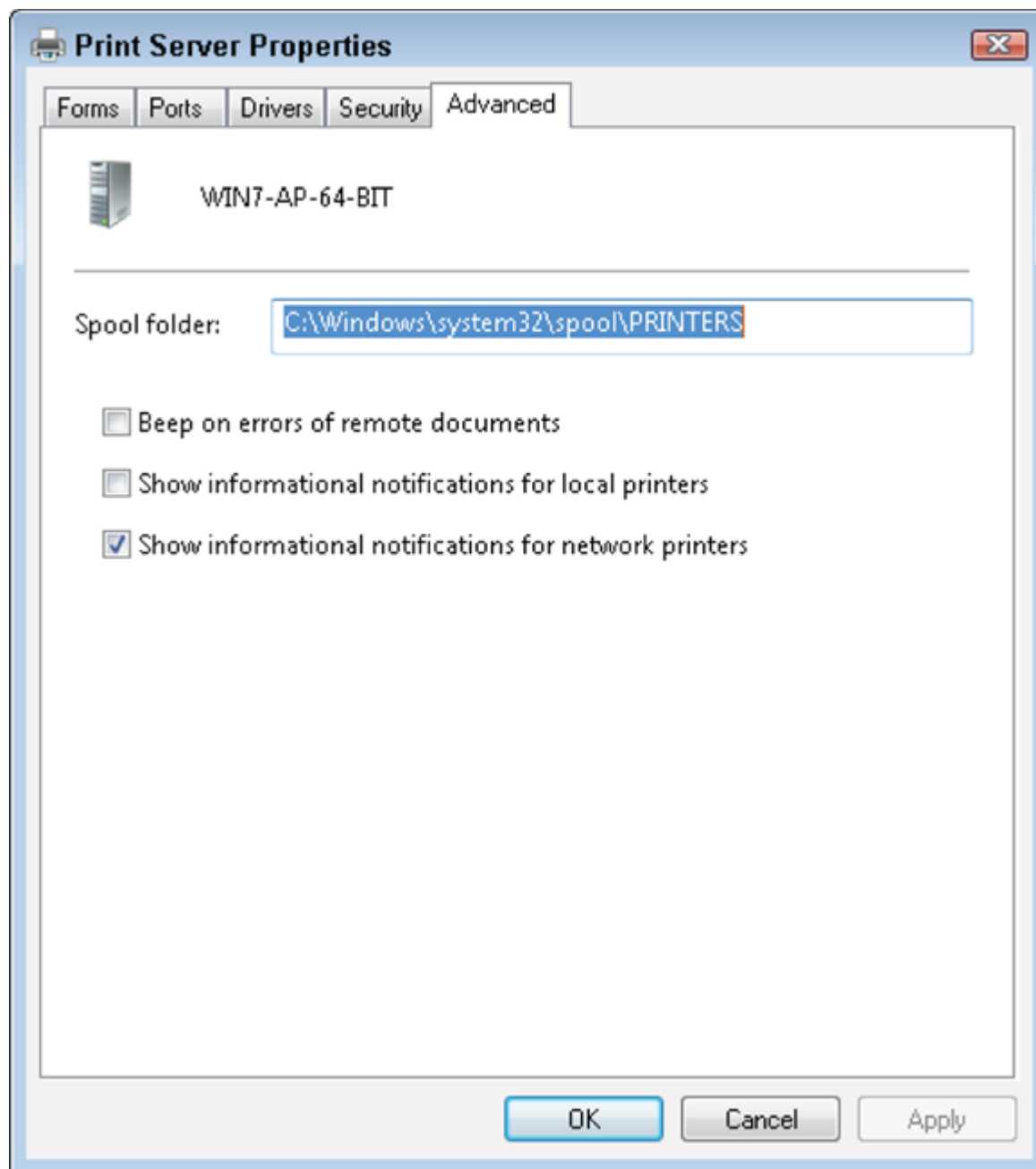
You can do several things to optimize your hard drives. The first thing is to choose the fastest possible drives for your system. If you can choose ATA 133 over ATA 66 or SATA 300 over SATA 150 or SSD over spindle drives, do so. Even within SSDs there are variations in access speed and improvements in technologies, which can make a wide variation in performance. Keep enough free space on your drives to allow for efficient defragmentation; Disk Defragmenter suggests 15 percent free space. If you have multiple drives in your system and you are suffering from a disk bottleneck, move some applications from one drive to another to better balance drive utilization.

## *Printers*

To optimize printing, here are a few things that you can do.

- » **Use current drivers for your printers.** Upgraded drivers often implement new features and are better optimized for your hardware. Most major manufacturers publish their printer drivers through Windows Update.
- » **Move your spool directory to a different drive.** Prior to sending data to the printer, the data is spooled to the computer's hard disk. In order to improve disk access, you should always try to place the spool directory on a fast disk that does not have competition from other applications or services that are running on the computer. For information about spooling, refer to Book 3, [Chapter 4](#).

To change the location of the spool directory on Windows 7, choose Start ⇒ Control Panel ⇒ Hardware and Sound ⇒ Devices and Printers. Then select a printer, choose Print Server Properties from the menu bar, and then click the Advanced tab, as shown in [Figure 3-17](#). From there, you can change the spool folder path.



**FIGURE 3-17:** Changing the spool folder path may improve printing performance.

If you are just printing the odd document, optimizing the printing process is not an issue. But if you are using a computer as a print server for an office and interfacing with multiple printers, these steps improve your printing performance.

### *Temporary files*

Many applications create temporary files, which are kind of like a scratchpad that is a working area for data. An application uses a temporary file to store data that it is working with and then deletes the file when the task is completed. For instance, when you open a document in Microsoft Word, Word creates other files in the same directory that start with a ~ character. These other files are temporary files, which hold changes to the original document as well as automatic recovery information. When you close the document, Word deletes these files — or, at least, it is supposed to.

It is the job of each application to delete its temporary files when they are no longer needed. Windows uses the environment variables of %temp% and %tmp% to point applications to the temporary directory. The default location for the temporary directory is in the user's profile, using the path %USERPROFILE%\AppData\Local\Temp.

Having the temporary file directory in the user's profile means that a temporary directory exists for every user on the computer. You can modify each user's temporary directory settings to point to a single location and schedule a task to run a command like `C:\Windows\system32\cmd.exe /c del /s /q c:\temp` when the computer starts up. Applications are supposed to clean up their files, but after a period of time, you will likely have several files in your temporary directory. You can use the Windows Disk Cleanup utility to delete temporary files, as well as other files not needed on your hard drive.

To get to Disk Cleanup, choose Start ⇒ All Programs ⇒ Accessories ⇒ System Tools ⇒ Disk Cleanup button. On a Windows 8.1 or Windows 10 computer, you will get to Disk Cleanup by clicking Start, typing **Free**, and then selecting “Free up disk space by deleting unnecessary files.” A Disk Cleanup dialog box will open, allowing you to choose the drive to clean up, and after scanning your disk the dialog box will change, presenting you a list of items that can be cleaned off your hard disk, such as temporary Internet files, items in the Recycle Bin, and temporary files. Place a check in the box next to any items you want cleaned, click OK, and then click Yes in the confirmation dialog box.



## Services

Each *service* represents an application running on your computer. The more applications that are running, the fewer system resources you have available for other applications or processes. To improve overall resource availability and system security, disable any services that are not required. You can see a list of all system services through the Services Administrative tool. Choose Start ⇒ Run (or Search Programs and Files) and type **services.msc**, or locate it in the Administrative Tools folder, which is found in the Control Panel folder. The Services Administrative tool lists the following information:

- » **Name:** The name of service
- » **Description:** A brief description of what the service does
- » **Status:** Tells you whether the service is currently running
- » **Startup Type:** Tells you whether the service startup is Automatic or Manual, or whether the service is disabled
- » **Log On As:** The user credentials used to start the service

Most services start as the Local System, which is the computer's own account.

When you select a service, you can read its description on the left of the window. With that information, you might be able to decide whether you need that service running. To test whether you need a service, turn it off, right-click the service name, and choose Stop. You can then tell quickly whether you need that service because something you use will stop working. When you turn off services by choosing Stop, the service restarts when you reboot. To have a service remain stopped after a reboot, right-click the service name and choose Properties; to open the Service Properties dialog box, choose Manual from the Startup Type drop-down menu, and click then OK to close the dialog box.

Prior to randomly turning off services, you can check whether the service is required by using Internet resources, like the Microsoft website, which will provide detailed descriptions of what most services are used for. If you *still* cannot decide whether a service is required, disable the service

on a test computer and see what happens. [Table 3-2](#) summarizes the major services that are part of Windows.

**TABLE 3-2 Windows Services**

<b><i>Name</i></b>	<b><i>Description</i></b>
Computer Browser	Maintains a list of other computers on the network
Windows Error Reporting Service	Allows error reporting to user and to Microsoft
Windows Event Log	Logs messages issued by Windows-based programs and components into logs viewed with Event Viewer
Windows Search	Indexes contents and properties of files
Network Connections	Manages the Network and Dial-Up Connections folder
Performance Logs and Alerts	Collects performance data from local or remote computers and generates alerts, based on settings found in Performance Logs and Alerts
Print Spooler	Loads files for deferred printing
Secondary Logon	Allows starting of applications using an alternate set of user credentials
Security Center	Monitors system security settings and configuration
Server	Supports file and print sharing over the network
Task Scheduler	Enables configuration and scheduling of automated tasks
Terminal Services or Remote Desktop Services	Holds base multiuser components used by Remote Desktop, Fast User Switching, Remote Assistance, and Terminal Server
Volume Shadow Copy	Allows Volume Shadow Copies used for backup and other purposes
Windows Firewall/Internet Connection Sharing (ICS)	Provides firewall and Internet gateway services, such as name resolution, network address translation, and intrusion prevention services
Windows Installer	Base Windows component that allows for the installation of MSI files
WLAN Autoconfig	Provides a standard configuration interface for 802.11 adapters

<b>Name</b>	<b>Description</b>
Workstation	Creates and maintains client network connections to remote computers

Properties can be set and managed for services. To change the properties of a service, open the Services Administrative Tool, as previously mentioned; then locate and select the service you want to modify or view settings for and then right-click Properties. This opens the service Properties dialog box, which has four tabs: General, Log On, Recovery, and Dependencies.

### ***General tab***

On the General tab, you can see basic information for the service, and, most of the time, this is the only tab you need to use. This shows you the display name used in the Services tool, as well as the path to the executable that is run to start the service. A startup type can be set to Automatic, Manual, or Disabled. The Automatic settings start the service on computer reboot; Manual allows it to be started by using the `net start` command or the Services tool; Disabled disallows the service to be run at all.

There are also service control buttons to start, stop, pause, and resume a service. Start and Stop are self-explanatory and are supported by all, but some services support Pause and Resume. Pause typically prevents new requests from being processed by the service, but will allow existing requests to be processed. Resume restores a paused service to normal operation. One case in which you might use this is with the Server service, which allows people to access files on your computer from across the network. Stopping the service disconnects all users. Pausing the service prevents new users from accessing files on your computer, but people who already have that connection open are able to finish their work. After all users have completed their work and have disconnected from your computer, you can complete what you were intending to do, which might be to stop the service, make a configuration change, and restart the service.

Some services accept startup parameters in the same way that you can pass parameters to other applications. When a service is stopped, you can add or change the Start parameters, and then start the service.

### ***Log On tab***

All services are programs, and all programs on a Windows NT-based computer will run using security settings of a user account. Most services run using the OS's account, also called Local System; however, you might want a service to run using a different account so that you can restrict what the service can do or so that the service can interact with other computers on the network.

### ***Recovery tab***

The Recovery tab allows you to deal with what to do when the service stops unexpectedly. Three drop-down menus enable you to specify an action for the First failure, Second failure, and Subsequent failures. For each menu, you can choose Take No Action, Restart the Service, Run a Program, or Restart the Computer. Windows will attempt to restart the service twice before taking no further action.



**TIP**

If a service fails for an unknown reason, you can set the service to restart on failure while you are trying to find the root cause, which might be enough to continue to provide the functionality required.

If you specify to run a program, you can use the bottom of the Properties dialog box to specify what program or batch file you want to run and the parameters to pass to the program. The program or batch file may be used to automatically fix a known problem or to send an email or alert to the administrator of the computer.

If you choose to restart the computer, click the Restart Computer Options button at the bottom of the dialog box to set the delay for the reboot, and a message to send to people connected to the computer.

Windows Vista introduced the Enable Actions for Stops with Errors option, which deals with a rare situation where services may stop

normally, but fail to set the `ERROR_SUCCESS` flag. By not setting the success flag, it makes it look like they had failed, while they had actually shut down properly. To deal with this unique situation, and to prevent inappropriate restarts of the service, this setting is off. But if you suspect that this is preventing an expected restart of your services, enable this feature.

Finally, the Recovery tab enables you to specify the number of days at which you will reset the failure counter and the time to wait before restarting a service.

### *Dependencies tab*

Some services require that other services are running prior to starting up. If you try to start a service that depends on other services not running, the required services will also be started. The Dependencies tab allows you to see both services that the selected service requires as well as what other services need the selected service.



**TIP**

One service that I often disable on systems with limited resources is the Themes service. This service is responsible for drawing windows with rounded corners and most of the graphical enhancements. All these items take processor time and memory to render for the user. By disabling the Themes service, these enhancements are automatically disabled. There may be some cases in which a user might feel that this service is required, and the same can be said of any service. For instance, an anti-spyware service running in real-time mode, checking each file that is accessed on your hard drive is a good service to have running on a computer connected to the Internet and used for web browsing, but this same service may be of limited use on an isolated computer with no Internet access.

### *Startup*

When your computer starts up, it loads all its services as well as any applications that are referenced in the Run Registry keys and the Startup

group in your Start menu. The Run Registry keys include:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run  
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce  
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx  
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run  
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
```

These items represent applications running on your computer. Many of these items, as well as some services, are responsible for the ever-growing string of icons next to your clock in the system tray. Each is a running application or process that takes system resources away from other applications or processes.

Many icons in your system tray have preferences or options that allow you to stop the background process from running. If you disable this service, some applications might take longer to load. For instance, Sun's Java and Apple's QuickTime use the startup Registry key to place one of their startup applications in the system tray, and they use the application to prelaunch their main application environments. For example, when you launch a QuickTime movie, QuickTime is already running and only needs to open the media file. If this process were not running, you would have to load QuickTime into memory before running the media file. On systems with limited resources, you want to remove many of these preloaded components to free the critical resources they use. Even though each icon represents a small amount of resource, they all make up the straws on the camel's back, and you never know where the breaking point is.

## ***GUI enhancements***

There are many GUI enhancements that have been added to the Windows OS over time. These enhancements have made the user interface more attractive, and in some cases more functional — but always at a cost of resource utilization. On computers that are underpowered, turning off these enhancements can provide a significant performance increase. These enhancements include:

- » Windows Aero in Windows 7
- » Advanced Themes

## » Visual Effects

Each of these enhancements can be disabled to improve the overall performance of the computer, but at a loss of the features provided.

### *Windows Aero*

The Aero desktop experience provides much of Windows 7's eye candy in features such as Windows Flip, Windows Flip 3D, Glass effects, and the live taskbar thumbnails. All these features make the later Windows OSes a little nicer to use, but each feature consumes system resources.

To disable the Aero desktop in Windows 7, use the following steps:

1. **Right-click an empty spot on your desktop and choose Personalize.**
2. **Choose any desktop theme, other than the ones in the Aero Themes section.**
3. **Close the Personalization control panel.**

### *Advanced Themes*

Windows has default desktop themes that present windows and dialogs using windows with rounded corners, and other window dressings.

Displaying windows this way consumes more system resources.

Microsoft provides a theme called Windows Classic, which does not use these appearance features.

To change your theme using Windows 7, follow these steps:

1. **Right-click an empty spot on your desktop and choose Personalize.**
2. **Choose any desktop theme from the Basic and High Contrast Themes section, other than Windows 7 Basic.**
3. **Close the Personalization control panel.**

To change your theme using Windows 10, follow these steps:

1. **Right-click an empty spot on your desktop and click Personalize.**

2. **Click on the Theme link.**
3. **When the Theme Settings dialog opens, choose Windows from the Apply a Theme choices.**
4. **Close the Personalization settings panel.**

### *Visual Effects*

Visual Effects adds basic enhancements to the GUI, which include displaying window contents when moving or resizing windows, animating windows minimize and maximize actions, sliding taskbar buttons, and so on. Each of these niceties uses system resources. To turn off all visual effects, use the following process:

1. **Click Start, right-click Computer, and then click Properties. (On Windows 10, click Start, type System, and select System from the search results.)**

The System window opens.

2. **Click Advanced System Settings.**

The System Properties window opens.

3. **Under Performance, click Settings.**

The Performance Options window opens.

4. **Click the Visual Effects tab.**

5. **Select Adjust for Best Performance, and then click Apply.**

This process turns off all GUI enhancements that have been covered in this section thus far. If you only want to disable the rounded corners on your window and buttons, you only need to turn off Use Visual Styles on Windows and Buttons.

### *Windows Search or Indexing*

Indexing was first introduced in Book 5, [Chapter 4](#). This process reviews all data on your hard drive and builds a content index to allow you to search for the data much faster than would otherwise be possible — think of it like the index in this book. The process of building and maintaining



the index takes some of your system resources. This feature should be carefully evaluated before disabling, as it greatly improves search times.

In Windows 7, the Indexing feature was renamed to Windows Search. It not only indexes files, it also indexes emails, and most other content on your computer. If you stop the Windows Search service, then virtual folder views will not be available, and searching for files will use the slower item-by-item searching.

To stop the indexing process from running, you can go to the Services applet using the following process:

1. **Right-click Computer ⇒ Manage, or on Windows 10, right-click Start and choose Computer Management.**

The Computer Management window opens.

2. **Choose Services and Applications in the navigation pane, and then choose Services.**

3. **Locate Windows Search and choose the Stop button on the toolbar.**

If you want to prevent the service starting up during a restart of the computer, right-click on the service and choose Properties, then change the Startup type to either manual or disabled.

4. **Click OK to close the Properties window.**

## *Getting an A+*

This chapter reviews optimization of the Windows environment. Major points covered in this chapter include

- » Virtual memory and applications that access the paging file reduce performance.
- » Performance is increased by using the computer's faster interface available for a device, such as using FireWire rather than serial.
- » To improve performance, reduce the number of processes and services running.

- » Printers can be optimized by changing the location of the spool directory.

## *Prep Test*

- 1. You are working with a client and noticed that the disk activity light is constantly on. You need to find out what is causing the issue. What tools would you use to monitor disk I/O? (Choose all that apply.)**
  - (A) `replmon`
  - (B) `perfmon`
  - (C) `defrag`
  - (D) `taskman`
  
- 2. Your client has asked you to install more virtual memory on her computer. You need to explain to her exactly what virtual memory is. Virtual memory contains which item?**
  - (A) A special section of memory used for caching data
  - (B) An area of a hard drive for caching data
  - (C) An expanded memory PCI expansion card
  - (D) An extended memory PCI expansion card
  
- 3. What tool manages your virtual memory settings?**
  - (A) Memory Diagnostics
  - (B) `setver` command
  - (C) System Control Panel
  - (D) `mem` command
  
- 4. You are working with a customer who has reported performance problems with his computer. He is complaining that everything he tries to do on the computer takes a very long time. What two steps can you take to improve hard disk access? (Choose two.)**

- (A) Double the number of pins on his drive that are carrying data.
- (B) Defragment his drive.
- (C) Add a speed doubler to the drive bus.
- (D) Change to a faster bus architecture.

## *Answers*

1. **B, D.** Both Task Manager and Performance Monitor can be used to monitor disk input and output. Performance Monitor has more detailed results, while Task Manager provides only a few basic counters. *See “[Using Monitoring Tools](#).”*
2. **B.** Virtual memory is created by using a page file, which resides on a hard drive. Disk caching uses memory to cache data from the hard drive. *Review “[Virtual memory](#).”*
3. **C.** Virtual memory settings are managed through the System Control Panel. *Check out “[Virtual memory](#).”*
4. **B, D.** Two things that can be done to speed up disk access are defragmenting your hard drive and changing to disks that have faster bus architectures. *Peruse “[Hard disk drive and solid state drive](#).”*

# Chapter 4

## Using Windows-Based Troubleshooting Utilities

---

### IN THIS CHAPTER

- » Managing disk partitions
  - » Supporting system configurations
  - » Working with system and disk management tools
- 

This chapter is all about Windows-based troubleshooting utilities. These utilities fall into categories such as disk maintenance, configuration, diagnostic, and the ever-popular miscellaneous category. One major utility topic covered in this chapter is Registry-editing utilities. I examine this component thoroughly because this topic is often neglected. The content that you examine for Registry editing is more detailed than what you need for the A+ exams; when you finish this book, you'll have a great grasp on the capabilities of the Registry editing tools.

Another major topic I cover in this chapter is managing disk partitions and disk configurations. Knowing the differences between your RAID configurations and how to set up and configure your hard drive partitions is important in your knowledge to properly support systems.

As a CompTIA A+ Certified Professional, you will be called on from time to time to use the tools that are discussed in this chapter. So, in addition to knowing this content for the A+ exams, you need to understand these tools to do your job as a support professional.

## *Understanding Operating System Utilities for Disk Maintenance*

In this section, you examine different disk maintenance utilities that you can use to perform disk maintenance on your system. These utilities include Disk Management, `defrag`, and `chkdsk`. Each of these utilities serves a specific purpose for your operating system.

## *diskpart.exe and Disk Management*

Before you can store any data on your disk, you need to prepare the disk for use. You can use the `diskpart.exe` utility to prepare your disk to hold data if you are using the Windows Recovery Console or in Windows, but you will likely want to use Disk Management (`diskmgmt.msc`) if you are in Windows. I discuss the items to check in Disk Management in more detail in the section “[Working with Disk Management](#),” later in this chapter.

Data is stored on a disk in a partition, and that partition is assigned a drive letter. There are two main partitioning standards, Master Boot Record (MBR), which has been around since the start of modern computing, and GUID Partition Table (GPT), which has been supported since 2010.

Decisions around MBR partitioning were made when early computer disks were created, you were allowed to create only four partitions on a disk, and a table was created in the disk's BIOS to hold the partitioning information. The partition table has only four entries in it. The solution to the four-partition limit was to create a special partition, which is always stored in the last partition. This special partition is an *extended partition*, and it is designed to extend the number of drive letters you can associate with a drive. Remember that this is four, the same as the number of partitions. The extended partition does not have a drive letter associated with it, but rather allows you to create any number of logical drives within it, all of which do have drive letters. The data for the MBR is stored in the first sector of the disk. In addition to the limit on the number of partitions, there was one table being stored in a 512 byte sector, which in effect caps the maximum size of a partition at 2TB.

This process has been completely rebuilt with the GPT partitioning model. To not interfere with MBR data, the GPT is stored in the second

sector of the disk, and uses a minimum 16,384 bytes to store its data. This data starts with a GPT header and is followed by an array to store data for at least 128 partitions. Since the specification defines the minimum size of the array, it is possible to have a larger array supporting more than 128 partitions. The specifications for GPT are a subset of the UEFI specifications. If you are using 32-bit Windows 7, you are able access data on GPT partitions, but you are not able to boot from them; but all other current versions of Windows allow you also boot from the partitions if your hardware is using UEFI. The same can be said of FreeBSD 7.0 and up, Ubuntu 8.04 and up, Fedora 8 and up, and Mac OS X 10.4.0 and up.

Windows allows you to use either tool to manage your drives, either `diskpart.exe` or Disk Management, which is a *snap-in*, or a tool component for the Microsoft Management Console (MMC). Disk installation is covered in Book 2, [Chapter 5](#).

Knowing your way around `diskpart.exe` is still important because you may have to resort to using `diskpart.exe` to prepare a drive to store data during a Recovery Console session or to perform certain tasks that Disk Management does not support, such as extending a primary partition on a drive. In order to boot, a hard drive requires that one of its primary partitions be made active. Each partition that you create can then be formatted with a file system. Each file system has a maximum partition size, and Windows may have some imposed limits on top of that.



**TIP** You are able to use Disk Management to both extend and shrink partitions on a disk.

Each primary partition or logical drive that appears on your computer is still limited to the size specified by the file system that you use on it. FAT32 drives are limited to 2TB, but Windows limits the partitions to 32GB, and on MBR disks, even NTFS will be limited to 2TB; while on GPT disks you can use up to the theoretical limit of 16EB.



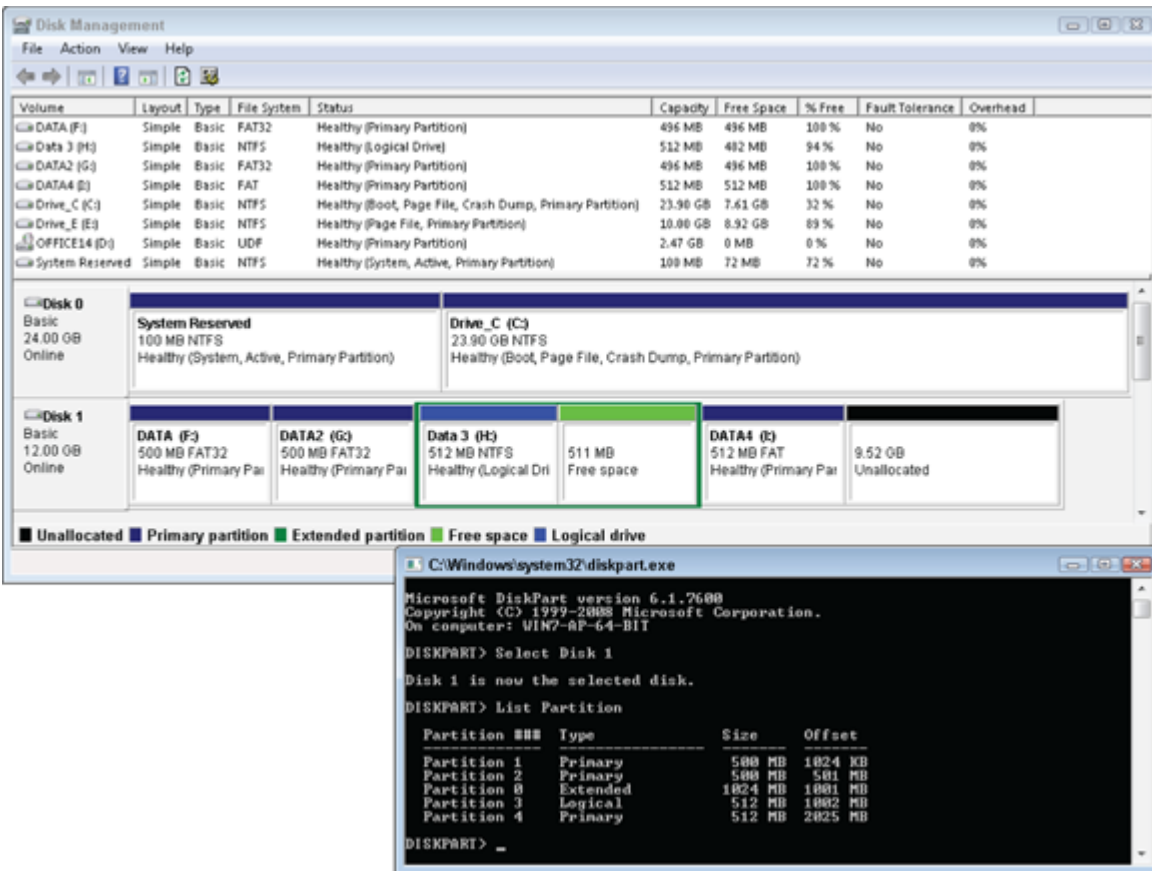
**TIP**

With MBR disks, you can boot only from an active partition, so if you don't set up an active partition on a new drive, you will not be able to boot from that drive.

If you use Disk Management, you can create up to four primary partitions on each drive. If you want to create an extended partition, you can create only three primary partitions. You also have the option of updating your disk to a *Dynamic Disk*, which eliminates the traditional limits to partition table entries by maintaining its own partitioning information in a separate location on the disk. Do not confuse Dynamic Disks, which Microsoft implemented prior to GPT, with GPT disks; these are two methods to get around the MBR disk limits.

Dynamic Disks do not have as many recovery tools as traditional Basic Disks and are compatible only with all modern Microsoft operating systems (OSes). Because of this recoverability aspect, you should avoid using Dynamic Disks unless they are necessary for your disk configurations.

In the Disk Management utility (see [Figure 4-1](#)), the entire contents of the disk partitioning scheme are visible in the display, and you are given control over the drive letters that are assigned.



**FIGURE 4-1:** Disk Management is more user-friendly than `diskpart.exe`.

## *defrag.exe and dfrgui.exe*

In this section, I discuss only the defragmentation options available to you in Windows because you will be tested only on the concepts of defragmentation or on the methods used to defragment disks within Windows.

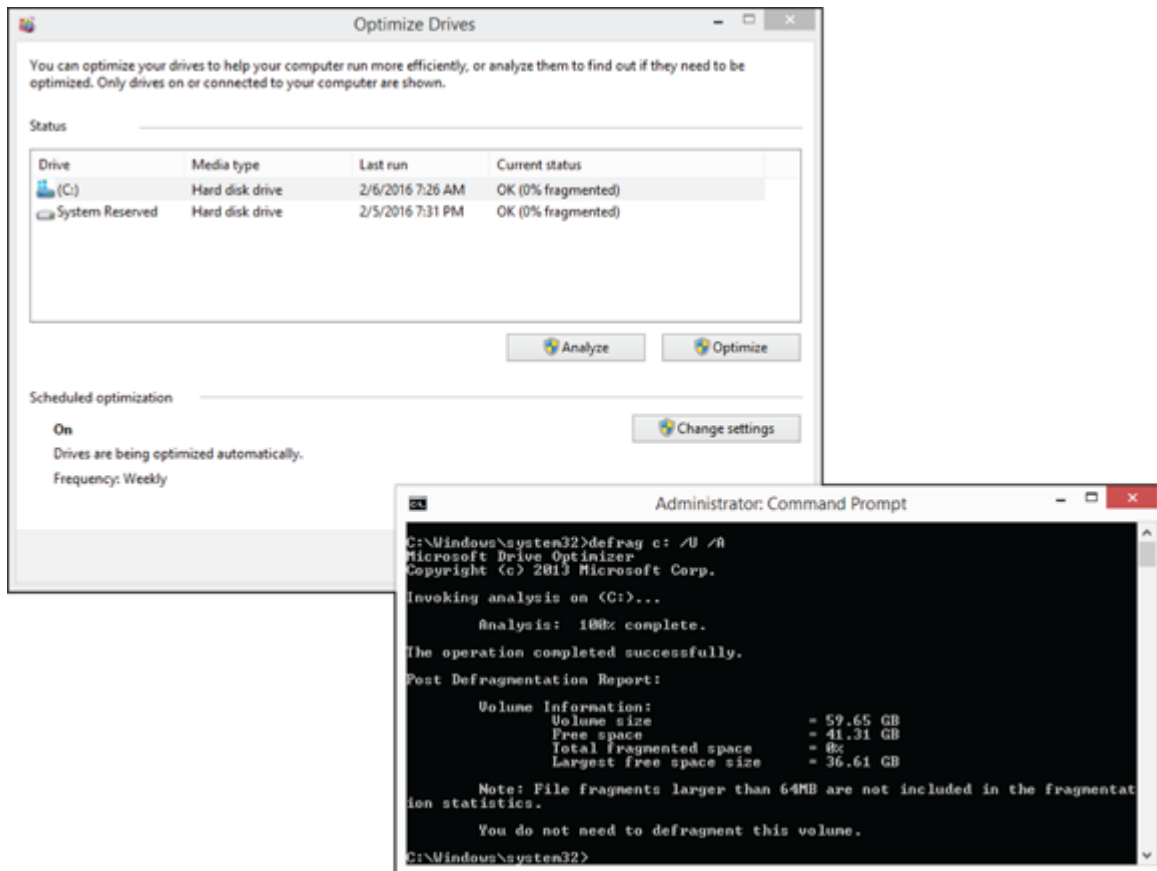
As you write data to your hard drive, it is always written into the largest area of available free space. When you delete files, though, areas of free space become broken up and scattered around your drive. Sometimes the largest area of free space is not large enough to hold the data being written. When this happens, the file is broken up into pieces — *fragmented* — to the areas of free space.

To “repair” the disk fragmentation, you can use `dfrgui.exe` or `defrag.exe`:



- » `dfrgui.exe` is the graphical defragmentation tool for Windows. In an effort to make names easier for end users, Windows 8.1 uses the display name of Optimize Drives when you launch this tool.
- » `defrag.exe` is a command line front end for the same tool.

Both tools for Windows 7 are shown in [Figure 4-2](#). While `dfrgui.exe` offers a simplified user interface, if you want to create a batch file or script to defragment your hard drive, you want to look at `defrag.exe`.



**FIGURE 4-2:** You have two interfaces to choose from to defragment your drives.

Defragmentation requires free space to do its job because it copies the files to new locations before removing them from the old locations. In addition to making all files contiguous, defragmentation attempts to consolidate most free space into a single unit, reducing how often new files are fragmented.



**REMEMBER** While the defragmentation process takes place, all files on your drive are read, and the system is checked for errors, in the same manner as `chkdsk.exe` (discussed in the next section).

Because the disk fragmentation utility rearranges the data on your drive and can therefore improve performance, it should be run periodically to ensure maximum performance of your computer. How you define “periodically” depends upon your system and how you use it. If your hard drive is extremely full (containing perhaps only a few gigabytes of free space), you should run `defrag.exe` as often as every few days. Comparatively, if you have a large amount of free space on your drive, files will take longer to become fragmented on your disk, and you might need to defragment your drive only once every month or two.



**TECHNICAL  
STUFF**

Defragmenting your data on a drive speeds access to files by eliminating the disk head seek time to move from one sector on the drive to another. When working with SSDs, there are no heads, and no seek time. You do get a benefit to moving blocks of data around, in fact, because the lifespan of an SSD is tied to an overall number of reads and writes, moving blocks of data will reduce the life of your drive. SSDs do benefit from index maintenance or garbage cleaning processes called TRIM. Starting with Windows 7, the Windows defragment tools perform a TRIM command when optimizing SSDs rather than a traditional data moving. When using Disk Defragmenter on Windows 10, you will not have the option to analyze SSD drives, but you will still be able to optimize the drives.

To open the graphical disk defragmenter, choose Start ⇒ All Programs ⇒ Accessories ⇒ System Tools ⇒ Disk Defragmenter, or if you are using Windows 10, choose Start ⇒ Windows Administrative Tools ⇒ Defragment and Optimize Drives. When you select a drive and then click the Analyze button, the defragmenter recommends whether you need to

defragment your drive. You can choose to use the Optimize button without performing the analysis. If you have noticed a degradation in performance, though, go ahead and defragment your drive. (Select a drive and click the Defragment button.) The recommendation to defragment your drive is made based on a threshold, and you may still benefit from defragmentation if you get near but not over the threshold.



**TIP**

You can use Scheduled Tasks to regularly run disk defragmentation by placing `defrag.exe` commands in a batch file; Windows has scheduling built right into `dfrgui.exe`. I cover scheduling tasks in the “[Miscellaneous Utilities](#)” section of this chapter.



**REMEMBER**

Free space and disk performance should be monitored to achieve an optimal level of performance.

### ***chkdsk.exe (Check Disk)***

The `chkdsk.exe` utility can identify potential problems with either your file system's allocation table or index, or the physical hard drive.

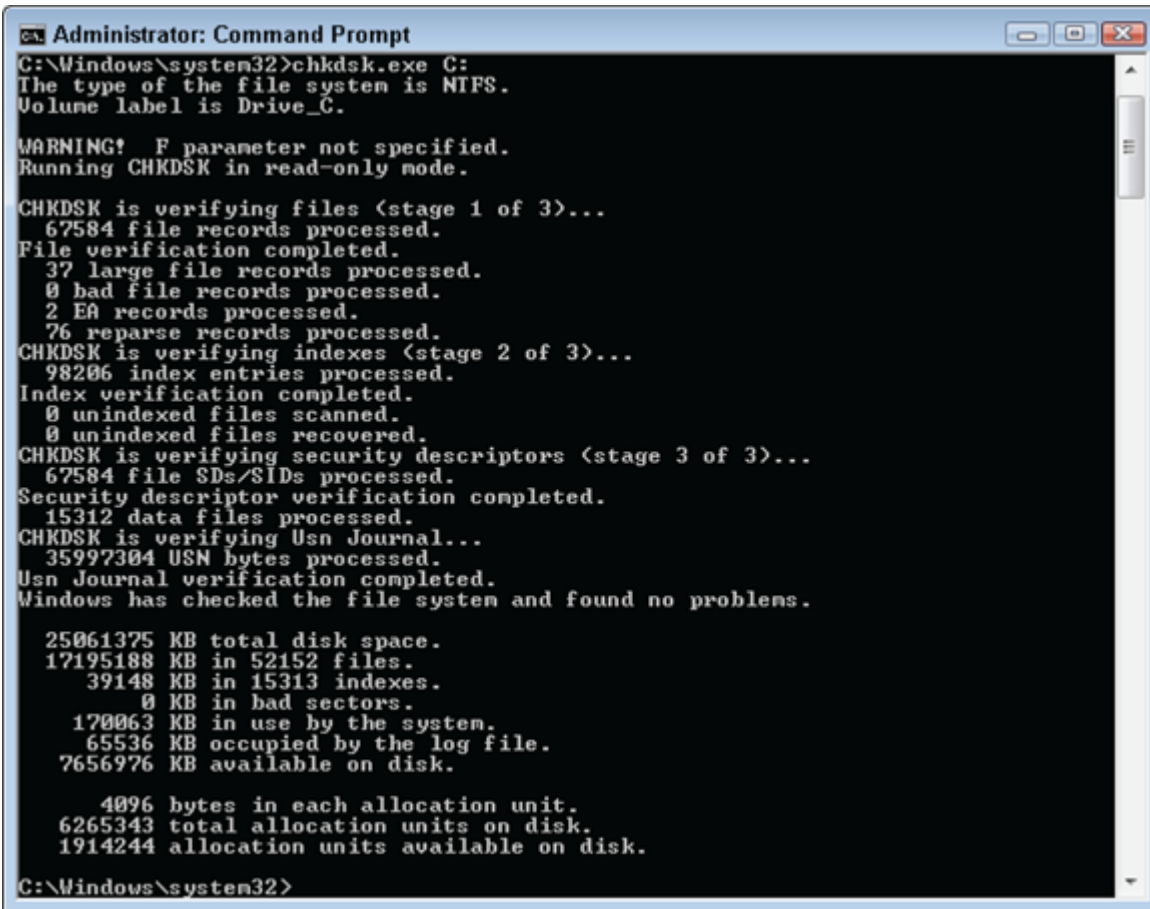
`chkdsk.exe` can be run from the command line or from the Tools tab of your disk drives' Properties. It has several options, of which the most important are

- » `/F`: Fixes errors found on the disk, rather than just identifying them
- » `/R`: Relocates bad sectors and recovers readable information
- » `/X`: Forces a dismount of the volume, which closes all open files

If you suspect that you have a disk problem, you should run a scan of your disk. However, because fixing errors requires exclusive access to the disk, you want to run `chkdsk.exe` in scan-only mode, which is the

default. If errors are detected, then you would want to specify /F and /X to correct any errors that are identified.

The system volume (C:) cannot be dismounted, so `chkdsk.exe` offers to schedule the scan during the next reboot of the system. On a system with a large C: drive, and depending on the number of errors, this scan can be very time consuming. The results of a scan can be seen [Figure 4-3](#).



```
Administrator: Command Prompt
C:\Windows\system32>chkdsk.exe C:
The type of the file system is NTFS.
Volume label is Drive_C.

WARNING! F parameter not specified.
Running CHKDSK in read-only mode.

CHKDSK is verifying files (stage 1 of 3)...
67584 file records processed.
File verification completed.
37 large file records processed.
0 bad file records processed.
2 EA records processed.
76 reparse records processed.
CHKDSK is verifying indexes (stage 2 of 3)...
98206 index entries processed.
Index verification completed.
0 unindexed files scanned.
0 unindexed files recovered.
CHKDSK is verifying security descriptors (stage 3 of 3)...
67584 file SDs/SIDs processed.
Security descriptor verification completed.
15312 data files processed.
CHKDSK is verifying Usn Journal...
35997304 USN bytes processed.
Usn Journal verification completed.
Windows has checked the file system and found no problems.

25061375 KB total disk space.
17195188 KB in 52152 files.
39148 KB in 15313 indexes.
0 KB in bad sectors.
170063 KB in use by the system.
65536 KB occupied by the log file.
7656976 KB available on disk.

4096 bytes in each allocation unit.
6265343 total allocation units on disk.
1914244 allocation units available on disk.

C:\Windows\system32>
```

**FIGURE 4-3:** Standard scans check the structure of the file tables.

In addition to issues with directory index entries and Master File Table (MFT) problems, `chkdsk.exe` looks for cross-linked files and orphaned directory entries or lost file fragments. The File Allocation Table (FAT) contains a pointer to the starting cluster for each file. As the file is read, a pointer at the end of each cluster identifies where the next cluster of the file can be found, with the last cluster of the file not containing a further pointer. From time to time, the pointer at the end of a cluster becomes

corrupted and starts pointing to the wrong location for the next bit of data. If the new location already contains file data (which contains a pointer to the next bit of data for a second file), you end up with two files using the same set of clusters.

When two files point to the same cluster (and clusters that follow), the situation is known as a *cross-linked file*. Depending on your outlook, you may choose to make copies of these files or to ignore them altogether. If you are a pessimist, you probably believe that both of these files are corrupt and probably garbage. If you are an optimist, you probably believe that one or both of these files are still readable and usable. There is no harm in having Check Disk create the files because your worst-case scenario will be that the files are of no use.

File fragments or lost chains, on the other hand, tend to be the leftover portions of cross-linked files (the portions of a file that would have belonged to a file had its clusters not been corrupted or lost). You have the option of either deleting these file fragments or converting them to files. If you choose to convert them to files, each chain is saved to the root directory with a name following the format `filennnn.chk` with an incremental number in place of the `nnnn`.



**TIP**

Although you have the option to convert lost file fragments to files, I have yet to see useful data recovered from file fragments, so you might as well delete them and free the space.

`chkdsk.exe` serves an important purpose on your system by ensuring data integrity of the files on your disk, and it should be scheduled to run periodically on important volumes because some disk corruption can be prevented if identified early.

## ***System Restore***

The System Restore process has been around since before Windows Vista, and it has been enhanced through each newer version of Windows. The System Restore process is tied together with the System Protection

settings. To access the System Protection settings, choose Start (or right-click Start) ⇒ Control Panel ⇒ System and Security ⇒ System, then click System Protection; on Windows 10, right-click Start ⇒ System ⇒ (scroll down) System info ⇒ System Protection. From the System Protection tab of the System Properties window, you are able to:

- » Configure the protection settings for your drives.
- » Specify the amount of space to be used.
- » Create System Restore Points.
- » Access the System Restore tool to restore your system to a previous point in time.

The System Restore process does not manage, back up, or restore personal files, and it is not intended to be used for that purpose; rather, it was designed to deal with operating system and program files. To learn more about the System Restore process, review Book 7, [Chapter 3](#).

## *Working with Disk Management*

When it comes to the day-to-day of working with disks, there are few things to be aware of in their management. This section deals with working with the items in Disk Management.

### *Drive status*

The first item to examine in Disk Management is the status of your disks. If you refer back to [Figure 4-1](#), you will see three important status indicators:

- » **Status column:** This is located in the top panel of the window and shows the current status of the drive, which indicates whether it is healthy, as well as what roles or functions it provides.
- » **Availability indicator:** This is located next to each drive in the bottom panel of the window and show the current availability status of the drive. Status could be Online, Offline, or Not Initialized.

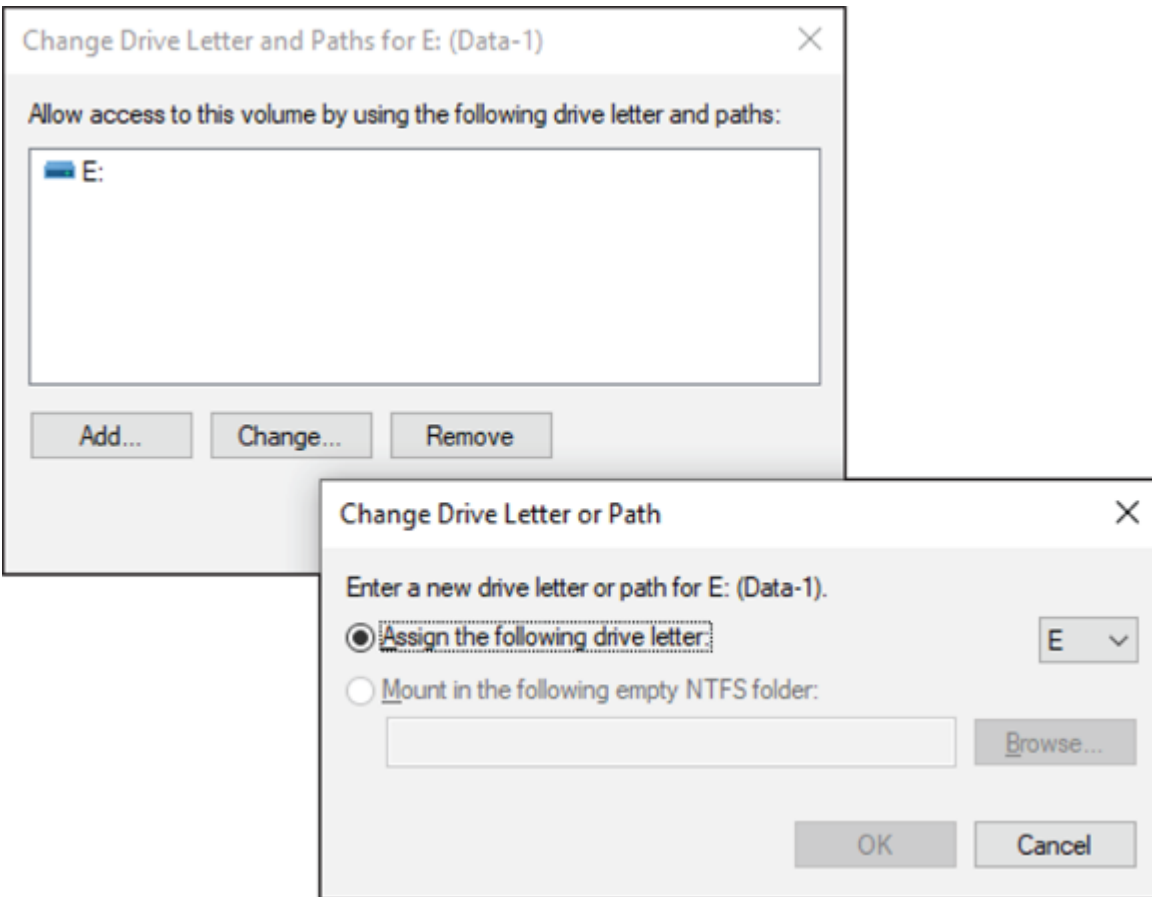
» **Disk Type:** This identifies the type of your drive, which may be Basic or Dynamic. Basic Disks are limited to four partitions, while Dynamic Disks do not suffer from this limit.

If the drive is marked as offline, then it was either manually set to offline or the drive has experienced some sort of failure. This failure may be recorded in the System Event Log, but your first attempt at troubleshooting should be bringing the drive back online by right-clicking on it and choosing Online.

### *Mounting and assigning/changing drive letters*

Mounting is the term use for connecting a drive letter to disk partition or network share. When dealing with Linux computers, you would attach a drive to empty folder by using the `mount` command, while with Windows computers you will perform that task through Disk Management or the `DiskPart` command.

To access files on a partition or volume, it requires that there be a drive letter assigned to it. Right-click on a volume and choose Change Drive Letter and Paths to access a window that allows you to add or change the assigned drive letter or mount the drive to an empty directory on another drive. This dialog can be seen in [Figure 4-4](#).

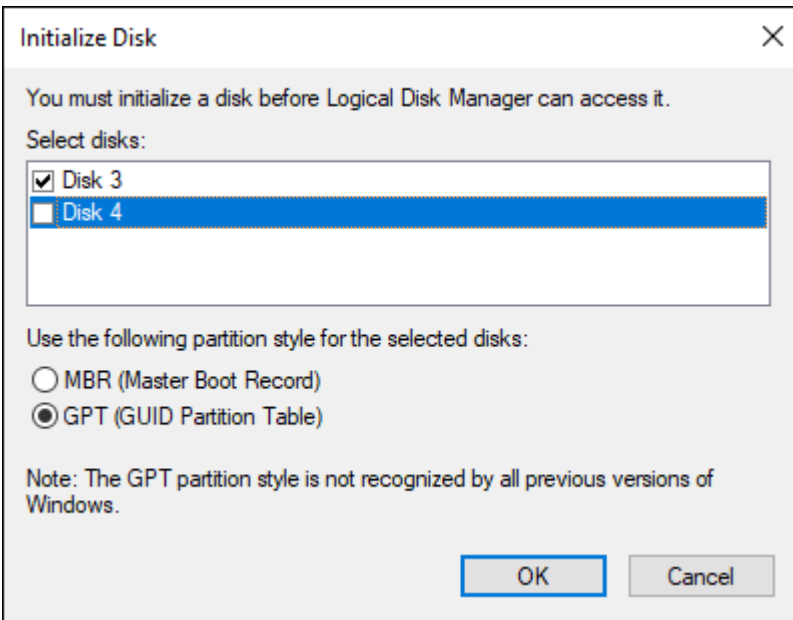


**FIGURE 4-4:** Assigning drive letters with Disk Management.

## *Initializing*

Before a drive can be used, it must be initialized. The initialization process on Windows will set the partitioning type, which is either GPT (GUID Partition Table) or MBR (Master Boot Record), and prepare the drive for use. GPT is the modern format and should be used if MBR compatibility is not required. After the drive is initialized, it will be automatically brought online. [Figure 4-5](#) shows one of two un-initialized drives being configured for a GPT partition table.





**FIGURE 4-5:** Disk initialization with Disk Management.

## *Creating partitions and adding arrays*

To create a new partition on your disk, right-click on the unallocated space on your disk and choose the partition type you want to create. If you choose anything other than New Simple Volume, you will be required to convert the disk to a Dynamic Disk. There are five types of partitions to choose from:

- » **Simple Volume:** This volume is a standard volume with no special functionality.
- » **Spanned Volume:** This volume uses space from two different drives and presents it to the Windows OS as a single drive with a single drive letter. This type of volume consolidates different sized spaces on different disks, but does not offer performance or data safety benefits of the other volume types.
- » **Striped Volume:** This volume takes equal space on two or more disks to writes data to each drive at the same time. This offers a performance benefit on reading and writing, but no data safety benefits. When data is written, it is broken into standard sized data blocks and written across all disks at the same time. This is the same

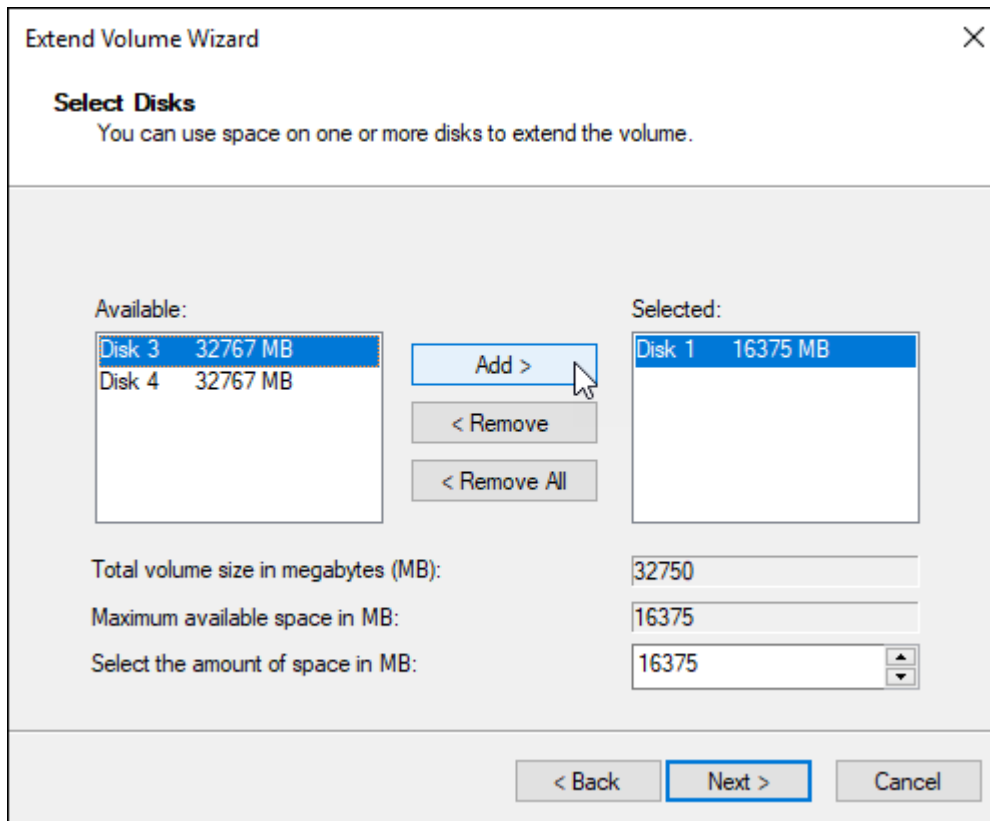
as RAID-0. Additional disks may be added after the initial creation of the volume.

- » **Mirrored Volume:** This volume takes equal space on two disks and writes the same data to each disk when saving data to the volume. This can offer performance benefits on data reads and offers data safety. Data safety is achieved as one of the two disks can fail, and all data will be accessible on the remaining disk. This is also called RAID-1. A mirrored volume can be created from any current disk volume by adding a mirror to it.
- » **Raid-5 Volume:** As the name suggests, this is a RAID-5 volume. This requires at least three disks and uses equal space on all disks. Data will be written to N-1 disks, with parity information written to the last drive. Each time data is written to the disk, it is broken into equal chunks and an equal-sized chunk of parity. Data is then written to all but one disk and the parity is written to the last disk. The parity data is moved each time to next disk in sequence. While calculating the parity takes a small amount of time, the performance loss from this is offset by the remaining data being written to several disks. When reading data, there is a performance benefit. Greater than the performance benefit is the data security, as any one drive in the array can fail and all data will be accessible until the failed drive is replaced. The use of RAID-5 offers more usable storage space when compared to a mirrored volume, since a mirrored volume provides storage on 50 percent of the disk space, and RAID-5 only loses the space equal to one disk.

## *Extending partitions*

When you create a partition on a drive, the partition may take up the entire drive, or it may only take up a portion of the partition. If the partition only uses a portion of the partition, it may be increased to use up free space, which follows the partition. This is true of all Windows partition formats and disk types — Basic or Dynamic Disks. To extend a partition, right-click on a partition and select Extend Volume to open the Extend Volume Wizard, as shown in [Figure 4-6](#). This wizard allows you add space to the

existing partition and automatically attempts to use remaining free space on the same disk.



**FIGURE 4-6:** Extending a partition with Disk Management.

You can choose to add space from a different disk, and if you are currently using Basic Disks, you will be prompted to confirm converting all affected disks to Dynamic Disks. If you add space from multiple disks, you will be creating spanned volume.

## *Shrink partitions*

If a partition or volume is too large, you may choose to shrink it. There are some rules around shrinking a partition, but if the data that currently resides on a partition can be moved to the start of the partitions space, then the end of the partition can be changed to make the overall partition size smaller. To shrink a partition, right-click a partition and choose Shrink Volume. Then select the new size in the Shrink dialog box.

## *Splitting partitions*

Once a partition has been created, you are not able to split the partition into two smaller partitions using default Windows tools. If you need to split a partition into two pieces, you will need to make use of a third-party tool. Alternatively, you may choose to shrink a partition and then create a new partition in the free space.

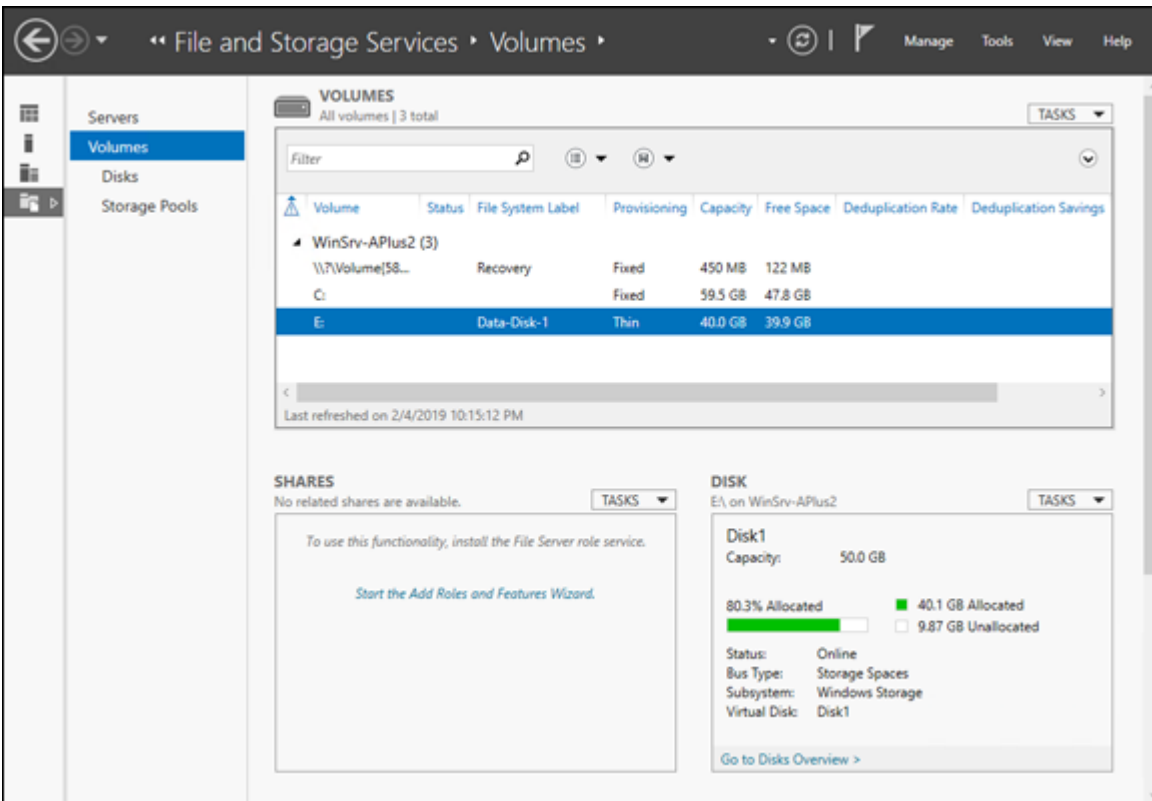
### *Adding drives*

When you add a drive to your computer, after initializing the drive, you will be able to make use of the drive as a new Basic Volume.

Alternatively, you may create a Mirrored Volume or add the disk to Spanned, Striped, or RAID-5 Volume.

### *Storage Spaces*

Windows Server 2012 R2 introduced Storage Spaces, which provides a great deal more flexibility in managing disks and storage. To access Storage Spaces, you will use the File and Storage Services Server Manager. This opens up the panels in Server Manager, as shown in [Figure 4-7](#). The storage options are similar to the previously mentioned RAID options, but with several benefits.



**FIGURE 4-7:** Storage Spaces provides storage flexibility.

The basic process for working with Storage Spaces follows this order:

- 1. Create a storage pool, which is a collection of physical disks.**

A *storage pool* allows you to collect disks into a single unit. You are also able to expand the pool as needed and to delegate management.

- 2. Create a virtual disk, which is also called Storage Spaces, and is the disk the Windows OS will see.**

The virtual disk is created in a storage pool and is assigned a storage layout type (simple, mirror or parity), provisioning type (thin or fixed), and a size. The storage layout is the RAID option for the disk, while provisioning allows for the disk to actively use up the space on the storage pool when fixed, or to only use the space equal to the data stored on disk in the case of thin provisioned disks.

A thin disk will start out using a minimum amount of space on the pool, and will grow as data is stored on the disk until it reaches its maximum size. Thin disks are like airlines overbooking flights, which

works well if all configured disks do not use their full configured size. On a single storage pool of 100GB, you could create ten 50GB thin-provisioned virtual disks, and while it may look from the OS that you have 500GB of space, you will be prevented from storing any more than 100GB of space. The idea being that you would monitor the space usage, and when the storage pool's space starts to run low, you would purchase and add additional disks to accommodate the space demand. The benefit being that you would not have to reconfigure the disks that were presented to the OS, and that this space management would happen behind the scenes.

### **3. Create a volume on the disk and format the volume.**

At this point in time, the volume would be available for use in the Windows OS.

In addition to thin provisioning disks, storage spaces support two key features:

- » Storage tiers allow a virtual disk to be composed of both fast SSDs and less expensive HDDs. As the SSDs fill, the least used data is automatically transferred to the HDD until it is needed. This allows a balance between performance and disk cost.
- » Enclosure awareness refers to external disk enclosures attached to a server. It allows the storage system to be aware of which enclosures your disks are located in, and it will balance data and parity information across enclosures to reduce risk of data loss when an entire enclosure is lost.

When working with Windows 10, there is a simplified set of options for Storage Spaces, which can be seen in [Figure 4-8](#). To access Storage Spaces on Windows 10, open the Start Menu, type **Storage Spaces**, and select Manage Storage Spaces.

**Create a storage space**

Enter a name, resiliency type, and size for the storage space

**Name and drive letter**

Name:

Drive letter:

File system:

**Resiliency**

Resiliency type:

**Size**

Total pool capacity:	94.4	GB
Available pool capacity:	93.7	GB
Size (maximum):	<input type="text" value="60.0"/>	<input type="text" value="GB"/>
Including resiliency:	90.0	GB

**Informational Messages:**

- A parity storage space writes your data with parity information, helping to protect you from a single drive failure. A parity storage space requires at least three drives.
- A storage space can be larger than the amount of available capacity in the storage pool. When you run low on capacity in the pool, you can add more drives.

**Buttons:** Create storage space, Cancel

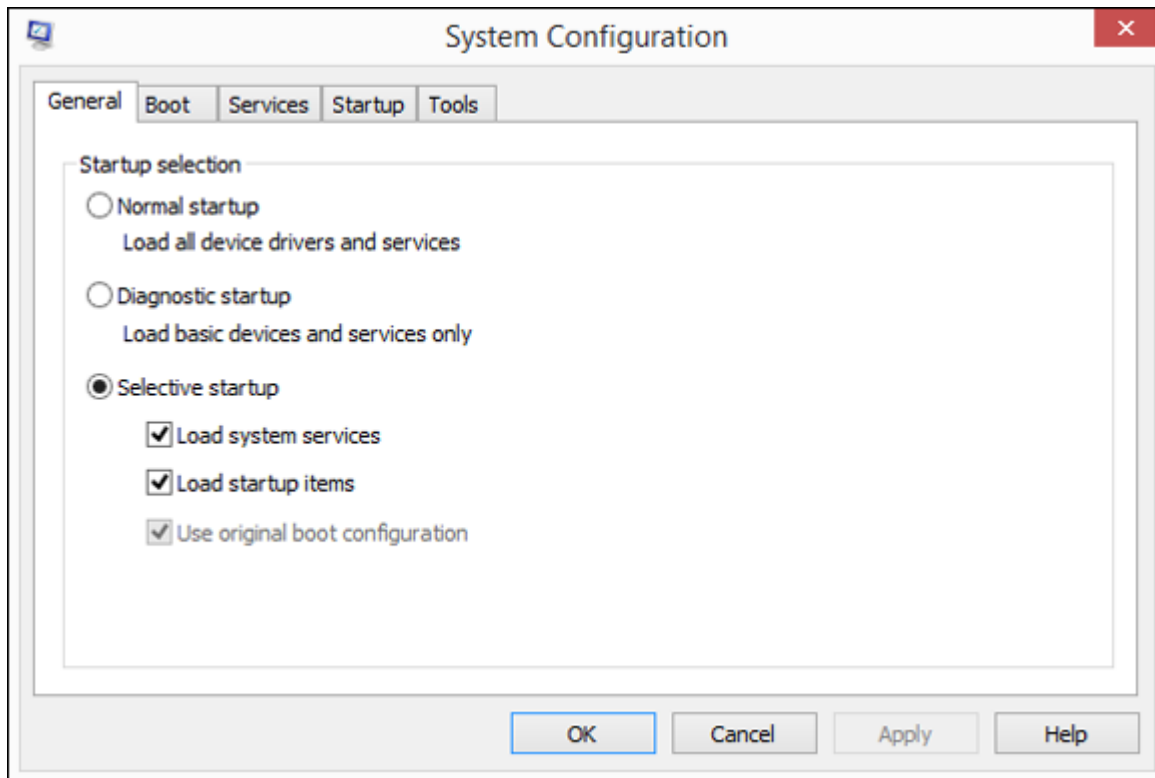
**FIGURE 4-8:** Creating a new volume using Windows 10 Storage Spaces.

## Configuration Utilities

This section discusses many of the configuration utilities that ship with the Windows OS. These utilities provide easy ways to modify configuration files and the Registry.

### *System Configuration utility (msconfig.exe)*

The System Configuration utility (see [Figure 4-9](#)) is a utility for maintaining settings on your Windows computer. To launch System Configuration, run `msconfig.exe`. This utility can change many aspects of your system startup. To use this utility, you need to be a member of the computer's Administrators group.



**FIGURE 4-9:** The initial window for System Configuration allows you to modify the basic system files.

The five tabs in this Windows utility allow you to launch the System Restore utility, expand files, perform selective boots, change the boot options in `boot.ini` or the BCD, and change the services and applications that are loaded at boot time. The five tabs are

- » **General:** Allows you to perform a custom startup, loading all device drivers and services, minimal device drivers and services, or a selective startup, choosing to load services and/or startup items.
- » **Boot:** Allows you to choose which installed OS you would like to boot, to boot Safe Mode with options, with or without a GUI, and



create a boot log. This page also allows you to make all your boot changes permanent.

- » **Services:** Allows you to specify which services you would like to load on the next boot of Windows.
- » **Startup:** Provides a link to the Startup section of Task Manager in Windows 8.1 and newer OSes, while Windows 7 provides a list of processes set to run automatically with Windows, allowing you to select which ones you would like to load on the next boot of Windows.
- » **Tools:** Provides a list of Windows tools which can be launched to resolve problems.

Use System Configuration to do the following:

- » Create custom startup configurations (for troubleshooting).
- » Perform a selective startup, which processes only some of the system files.
- » Expand operating system files from the OS CD.
- » Disable services or programs that have been added to the Run key of the Registry.

All the changes in the preceding bulleted list can be accomplished from within a simple Windows user interface, making System Configuration an easy configuration tool to work with.

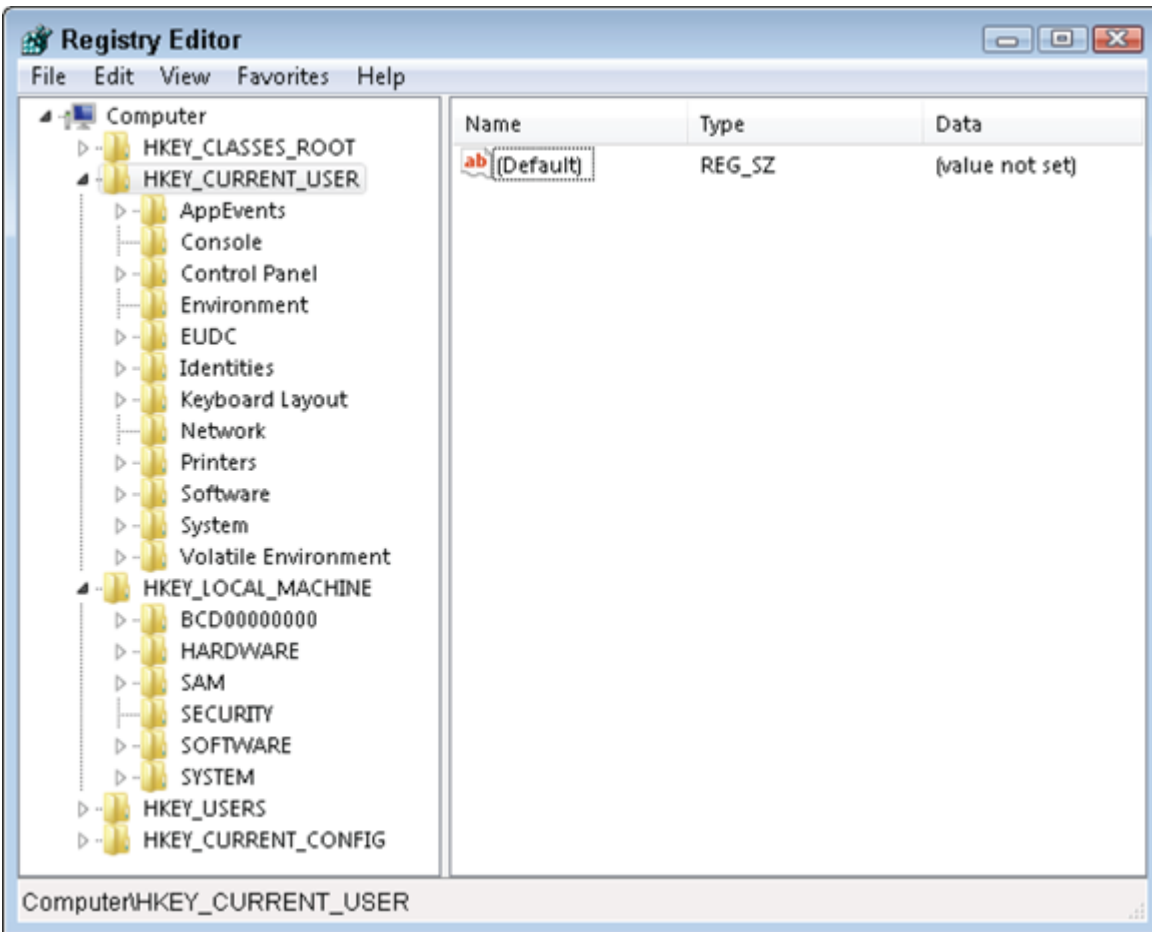
If you suspect that a computer problem is related to one of the components loaded at startup, this is the tool you want to use. If you can boot into Safe Mode but not perform a normal boot, you can use this tool to select which components you want to load on reboot. By disabling components, you should be able to narrow down which component is causing the problem, by performing multiple boots with different combinations of the items selected.

*regedit.exe*

If you have ever talked to anybody about the system Registry, you have probably been given a stern warning that this is not a place for the timid. The reason for this warning is that the Registry stores system-wide configuration information for almost all services on your computer. If you experience major problems with the Registry, you will likely have major problems with your entire computer.

The Windows Registry has five major subtrees, as shown in [Figure 4-10](#):

- » `HKEY_CLASSES_ROOT` contains information about all the file associations and registered file types that exist in your computer. This information is actually a copy of the information stored in the `HKEY_Local_Machine\software\classes` key.
- » `HKEY_CURRENT_USER` contains a subset of the information that is found in `HKEY_USERS` key, but contains only the information related to the current user. This key contains configuration information for the currently logged-on user. This information includes items such as Control Panel settings (including mouse acceleration and screen saver preferences) and user-related software settings for installed applications.
- » `HKEY_LOCAL_MACHINE` contains information about your computer. This information includes configuration information for hardware components and system settings for all software on the computer.
- » `HKEY_USERS` contains information for the currently logged-on user, as well as information for the default user and all other users who are logged onto the computer.
- » `HKEY_CURRENT_CONFIG` contains settings that are dynamically rebuilt on every boot of the computer, which is mainly composed of Plug and Play information.



**FIGURE 4-10:** Settings in the Registry cover most aspects of the system.

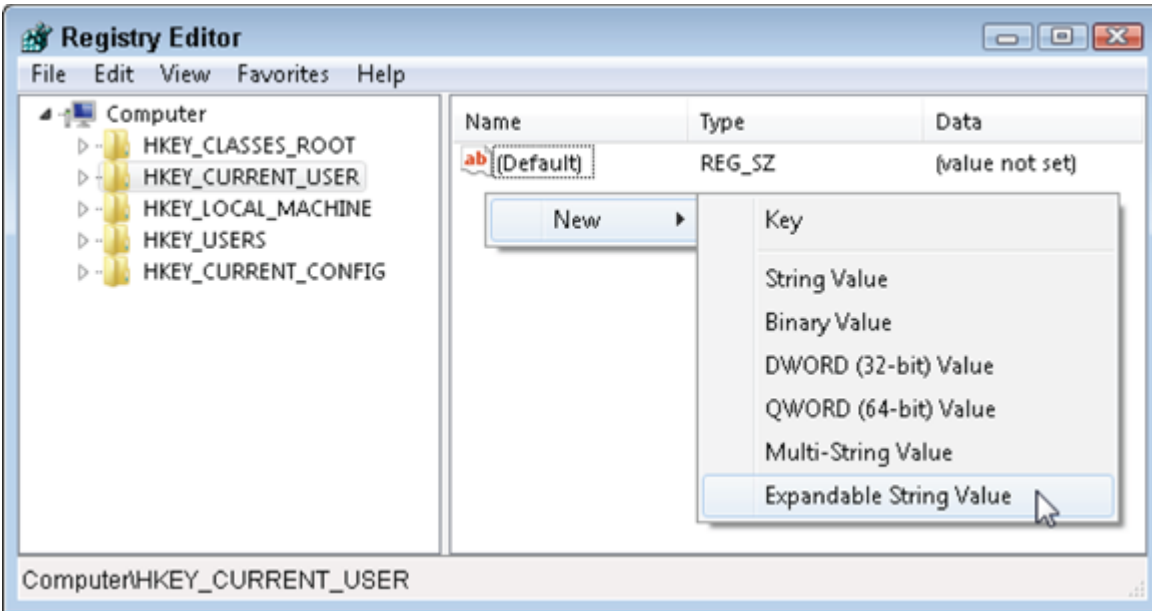
Of these subtrees, you really need to worry about only two:

`HKEY_CURRENT_USER` and `HKEY_LOCAL_MACHINE`. The information in the other subtrees is either duplicated within these two subtrees or the data cannot be modified.

All Registry entries are stored in a hierarchical tree. This tree contains several subfolders: *keys*. If you want to create new keys within the Registry, use the Edit ⇒ New ⇒ Key command. Every key within the Registry can store values. The Registry Editor contains six different types of values (as shown in [Figure 4-11](#)):

- » String
- » Binary
- » DWORD (32-bit)

- » QWORD (64-bit)
- » Multi-String
- » Expandable String



**FIGURE 4-11:** There are six basic data types for the Windows Registry.

Some hardware components or software components that you can install on your computer may create entries inside both `HKEY_LOCAL_MACHINE` and `HKEY_CURRENT_USER`. This makes sense if you think about applications like Microsoft Office. Microsoft Office creates entries in `HKEY_LOCAL_MACHINE` that relate to the location of Office components on the particular computer, such as the spell checker that can be found within `C:\Program Files\Microsoft Office\Tools`. At the same time, Microsoft Office installs entries in `HKEY_CURRENT_USER` that relate to the user configuration on the system. *User-related settings* are items such as the default Save As file type in Microsoft Word.



**TIP**

The Registry is an important part of your computer, and great care should be taken not to corrupt this database. Before you start doing any procedure that involves the Registry, make sure you have a clean

backup of the Registry. You can create this backup in a variety of ways, such as by exporting the Registry, by creating a System State backup, or by physically copying the files that make up the Registry.

To copy the files that make up the Registry, you need to know where the files actually are. `HKEY_CURRENT_USER`, the user portion of the Registry, can be found in your user profile directory. It will be named `NTuser.dat`. `HKEY_LOCAL_MACHINE` is actually composed of several files that are found in the Windows directory. These files should be backed up and restored by using the Windows backup program. With Windows, you can perform a System State backup or a Full backup.

Rather than backing up the entire Registry, though, you can be more selective and back up and restore individual keys within the Registry by using the Registry Editor.

To back up individual keys, follow these steps:

1. **Choose Start ⇒ Run (or Search or type on the Windows 10 Start Screen).**
2. **Type `regedit` in the Run dialog box that appears.**
3. **Click the key that you want to back up.**

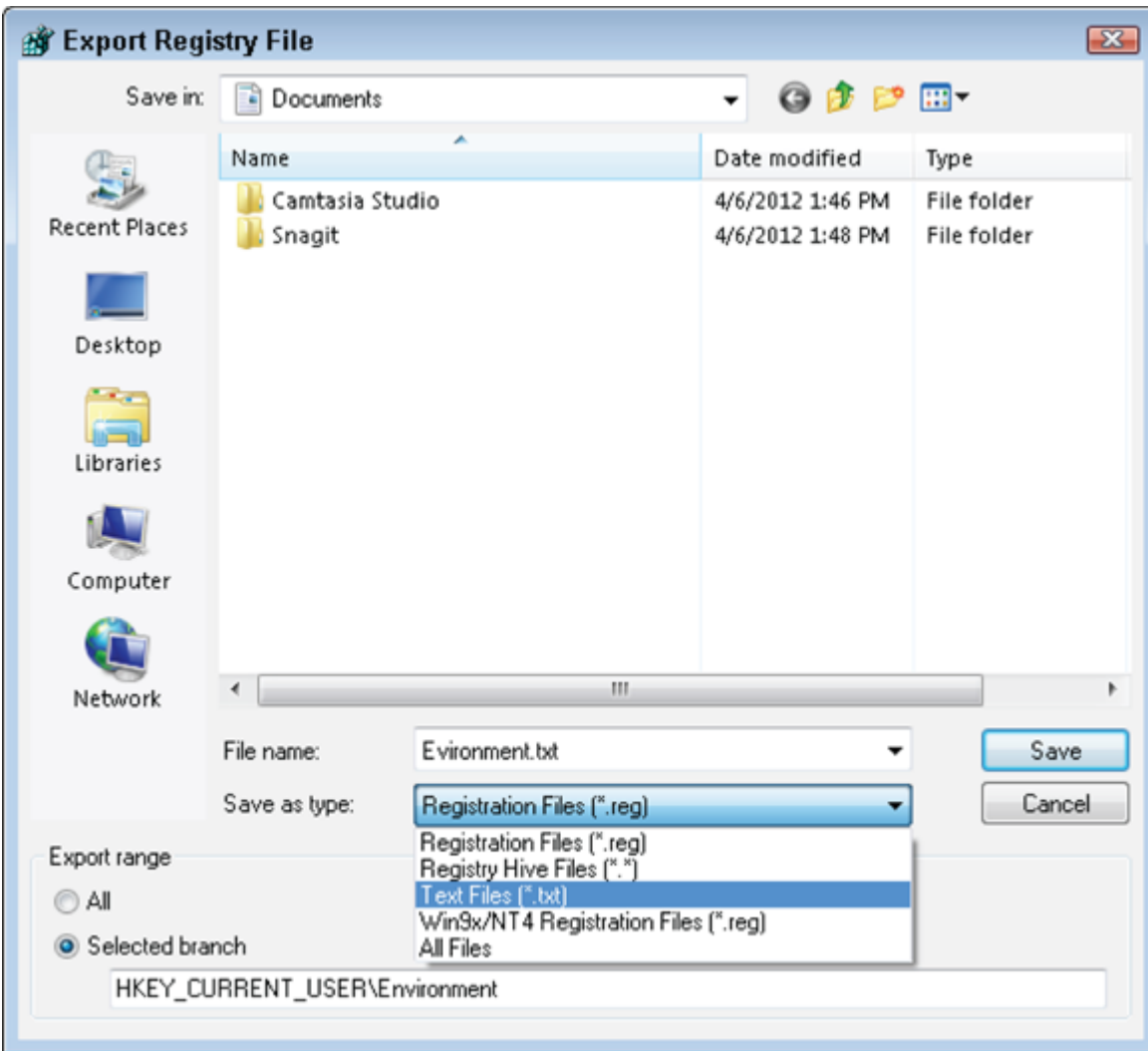
This highlights the key.

4. **Choose File ⇒ Export.**

The Export Registry File dialog box appears, as shown in [Figure 4-12](#). This dialog box looks similar to a standard Save As dialog box, with the addition of the Export Range panel at the bottom. The Export Range panel contains your selected branch within the Registry by default.

5. **Type a name for the file and choose a location for `regedit` to save it.**
6. **Click Save.**

The file is given the default `.reg` extension.

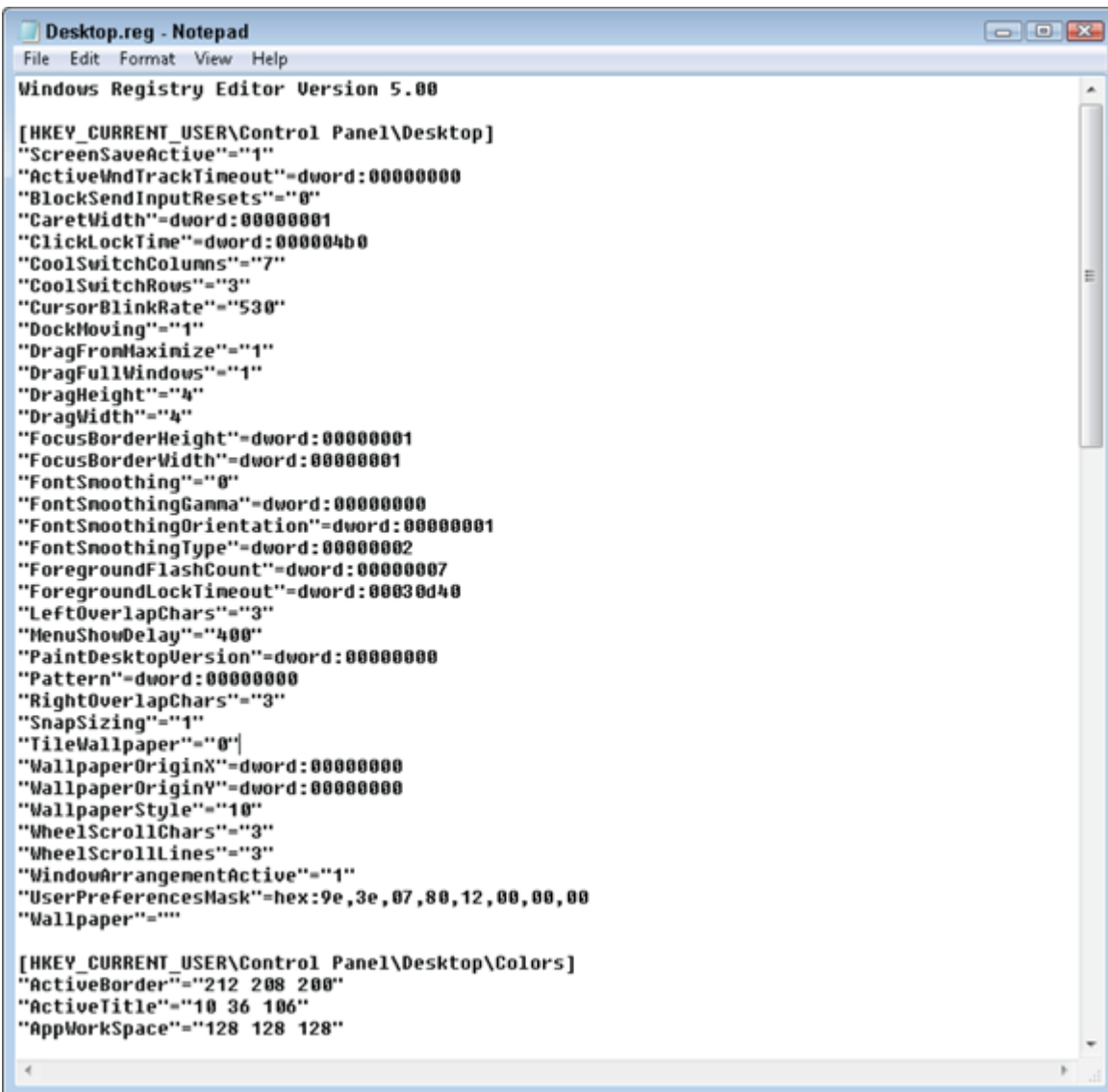


**FIGURE 4-12:** Export sections of the Registry as backup prior to editing.



**REMEMBER** Files that end in the `.reg` extension are Registry export files that you can edit with a text editor (as shown in [Figure 4-13](#)). REG files share the same basic structure as an INI file, which are sections defined by names in square brackets, containing value names and value data on either side of an equal sign. To import a REG file into the Registry, just double-click the file. To help prevent accidental importing of Registry files, Windows has added a safety feature: Windows prompts you to confirm that you would like to import the settings into your Registry, as shown in [Figure 4-14](#). After you

import the settings, a dialog box confirms that a file has been successfully merged into your Registry.



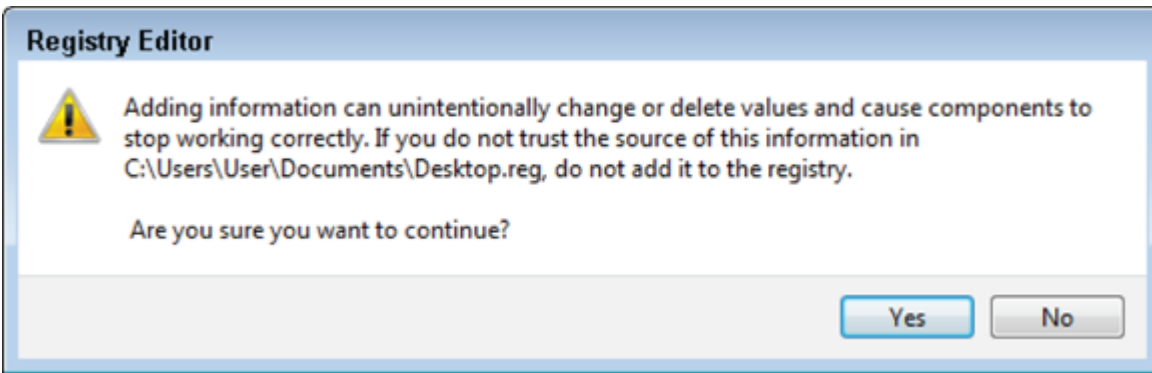
```
Desktop.reg - Notepad
File Edit Format View Help

Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Control Panel\Desktop]
"ScreenSaveActive"="1"
"ActiveWndTrackTimeout"=dword:00000000
"BlockSendInputResets"="0"
"CaretWidth"=dword:00000001
"ClickLockTime"=dword:000004b0
"CoolSwitchColumns"="7"
"CoolSwitchRows"="3"
"CursorBlinkRate"="530"
"DockMoving"="1"
"DragFromMaximize"="1"
"DragFullWindows"="1"
"DragHeight"="4"
"DragWidth"="4"
"FocusBorderHeight"=dword:00000001
"FocusBorderWidth"=dword:00000001
"FontSmoothing"="0"
"FontSmoothingGamma"=dword:00000000
"FontSmoothingOrientation"=dword:00000001
"FontSmoothingType"=dword:00000002
"ForegroundFlashCount"=dword:00000007
"ForegroundLockTimeout"=dword:00030d40
"LeftOverlapChars"="3"
"MenuShowDelay"="400"
"PaintDesktopVersion"=dword:00000000
"Pattern"=dword:00000000
"RightOverlapChars"="3"
"SnapSizing"="1"
"TileWallpaper"="0"
"WallpaperOriginX"=dword:00000000
"WallpaperOriginY"=dword:00000000
"WallpaperStyle"="10"
"WheelScrollChars"="3"
"WheelScrollLines"="3"
"WindowArrangementActive"="1"
"UserPreferencesMask"=hex:9e,3e,07,80,12,00,00,00
"Wallpaper"=""

[HKEY_CURRENT_USER\Control Panel\Desktop\Colors]
"ActiveBorder"="212 208 200"
"ActiveTitle"="10 36 106"
"AppWorkspace"="128 128 128"
```

**FIGURE 4-13:** All Registry export files share a structure that resembles Windows configuration files.



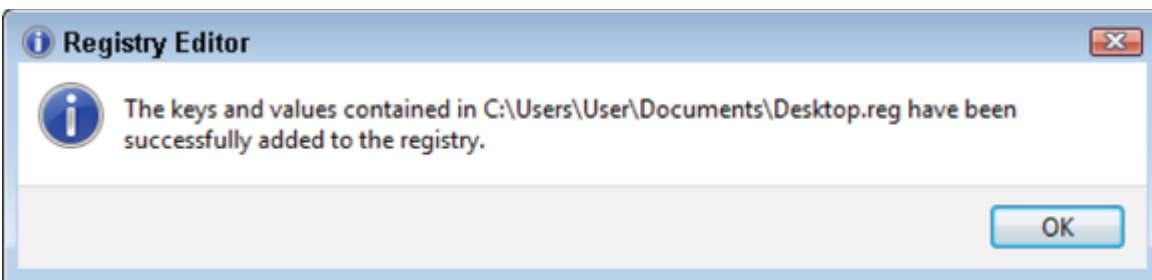
**FIGURE 4-14:** Heed the confirmation to limit accidental imports.



**TIP**

On Windows computers, REG files are automatically imported into your Registry if you double-click them. Rather than using the .reg extension on your files, you may choose to use TXT files. Files with the .txt extension can also be imported into your Registry by using `regedit.exe filename.txt` at the command line.

Periodically, REG files become corrupted from being edited with certain text editors, such as WordPad. This corruption occurs because some text editors add extended (invisible) characters into the text file that are not compatible with `regedit.exe`. The only editor that does not exhibit this behavior is Notepad. If you have a corrupted file, you can fix it by opening the file through Notepad, resaving the file, and closing it. When saving the file, ensure there is a blank line at the end of the file. Even if the file is corrupt, you still receive a dialog box stating the information has been successfully entered into your Registry, as shown in [Figure 4-15](#).



**FIGURE 4-15:** A successful Registry import.



When you work with Windows computers, you can use `regedit.exe` to connect to a remote Registry, which allows you to change the Registry settings on a remote computer without having to leave your own computer. To connect to a remote Registry from across the network, choose File ⇒ Connect Network Registry.

Another advantage of the Registry Editor is that you can load Registry hives. This capability becomes useful when you want to modify the entries for the default `ntuser.dat`. The default `ntuser.dat` is used as a template to create new user profiles for users who do not yet have a profile. You can find the `ntuser.dat` file for this default template account in `C:\Users\Default User\NTUSER.DAT`, and you can load this subtree or hive into `regedit.exe` and edit the settings for this default template.



**WARNING** Do not confuse this default user template with the default user in use prior to a user logging on to your computer. The Registry settings for the pre-logon default user are actually found in the Registry under `HKEY_USERS\DEFAULT`.

Another thing that you do with the Registry Editor is manage the security on Registry keys. To view or modify the security settings on a Registry key, first select the key and then choose Edit ⇒ Permissions. You can work with permissions on Registry keys only — not on Registry values.

To allow for command line editing of the Registry, Microsoft introduced `reg.exe` as a standard component of Windows; this is part of all current versions of Windows. This allows for loading and unloading of Registry hives as well as editing Registry keys and values.



**ON THE  
WEB**

Lab 4-1 will have you export your current desktop settings into a file and create a Registry file that is used to change wallpaper settings. Lab 4-1 can be downloaded from the companion website at [www.dummies.com/go/aplusaio](http://www.dummies.com/go/aplusaio).

## *regsvr32*

regsvr32 is short for register service and is a tool that is used to register and unregister Object Linking and Embedding (OLE) controls on your computer. These files can be contained in Dynamic Link Libraries (DLLs) or ActiveX Control (OCX) files.

When most applications run installation programs that include DLLs or other files that need to be registered, this is usually done as part of the installation process. However, when a problem occurs with the installation of a program, or if the developer has not created an installation package, you may find yourself registering and unregistering files by hand.

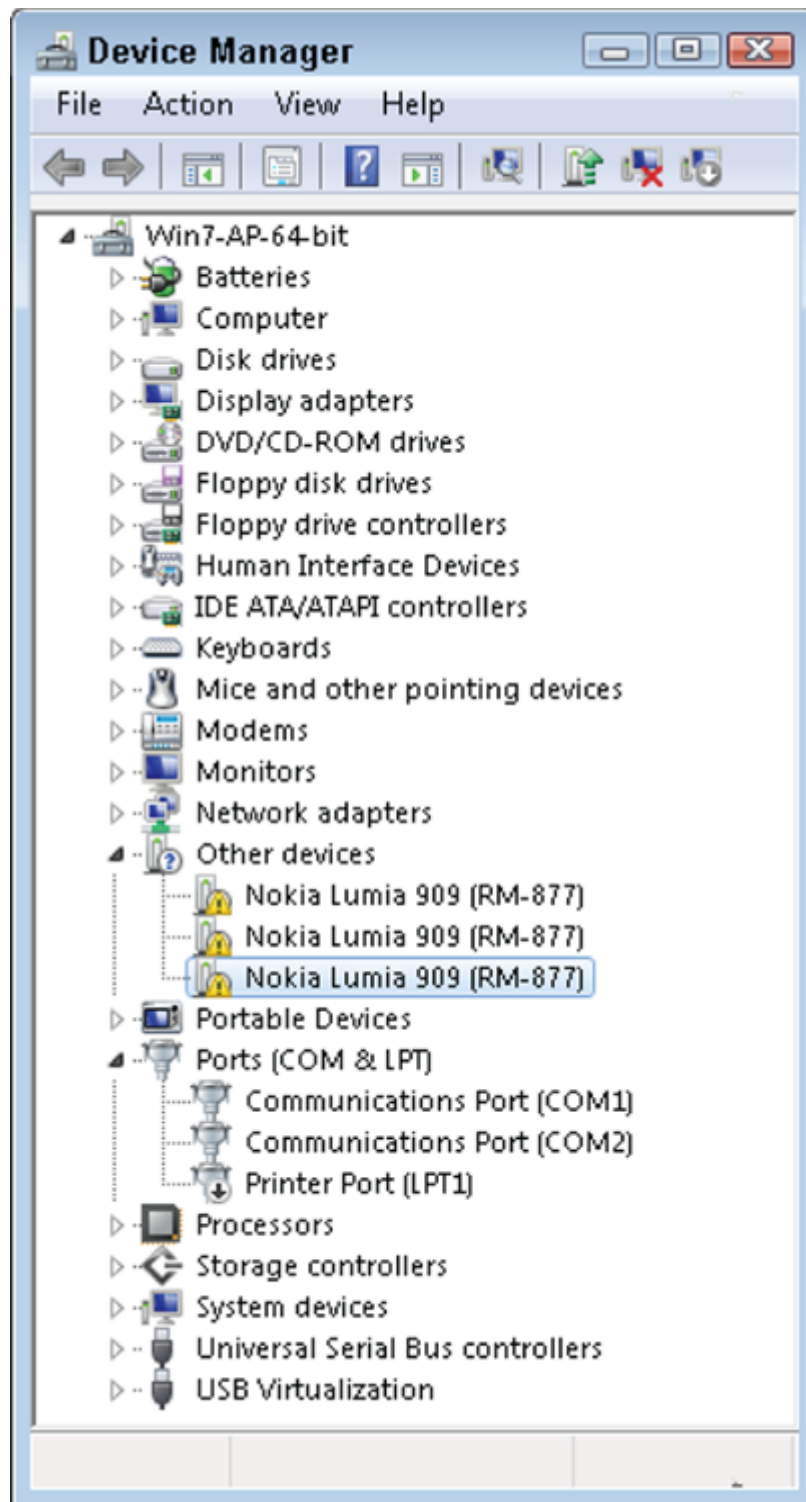
The easiest way to execute `regsvr32.exe` is to provide the name of the file that you want to register, such as `regsvr32 sample.ocx`. `regsvr32` does support switches, of which the two most common are

- » **/u:** Unregisters the service or server
- » **/s:** Performs a silent installation and suppresses all message boxes

## *Device Manager*

Device Manager (`devmgmt.msc`) is covered in more depth in Book 6, [Chapter 1](#). The primary job of Device Manager is, appropriately enough, managing devices. You can access Device Manager by clicking the Device Manager button on the Hardware tab of the System Properties window. Use Device Manager to remove devices from your system, configure drivers, configure hardware resources, and manage hardware profile settings.

In Device Manager, you can easily pick out the devices with hardware problems because they sport a symbol, such as a small downward arrow on the icon in the device tree. A red arrow identifies devices that are in conflict or are disabled. A yellow exclamation mark identifies devices that are not properly configured (as shown in [Figure 4-16](#)). You can use Device Manager to identify problems with your hardware; configure the drivers for the devices; and configure hardware resources, such as IRQs and I/O addresses.



**FIGURE 4-16:** When looking for malfunctioning devices, look for the warning symbols like the ones under Other Devices.

In addition to Device Manager, you can also find out information related to installed drivers on your computer or a remote computer by using the

`driverquery.exe` command. This command generates a list of driver names, display names, the type of driver (kernel or file system), and the driver date, which will be similar to the output shown here:

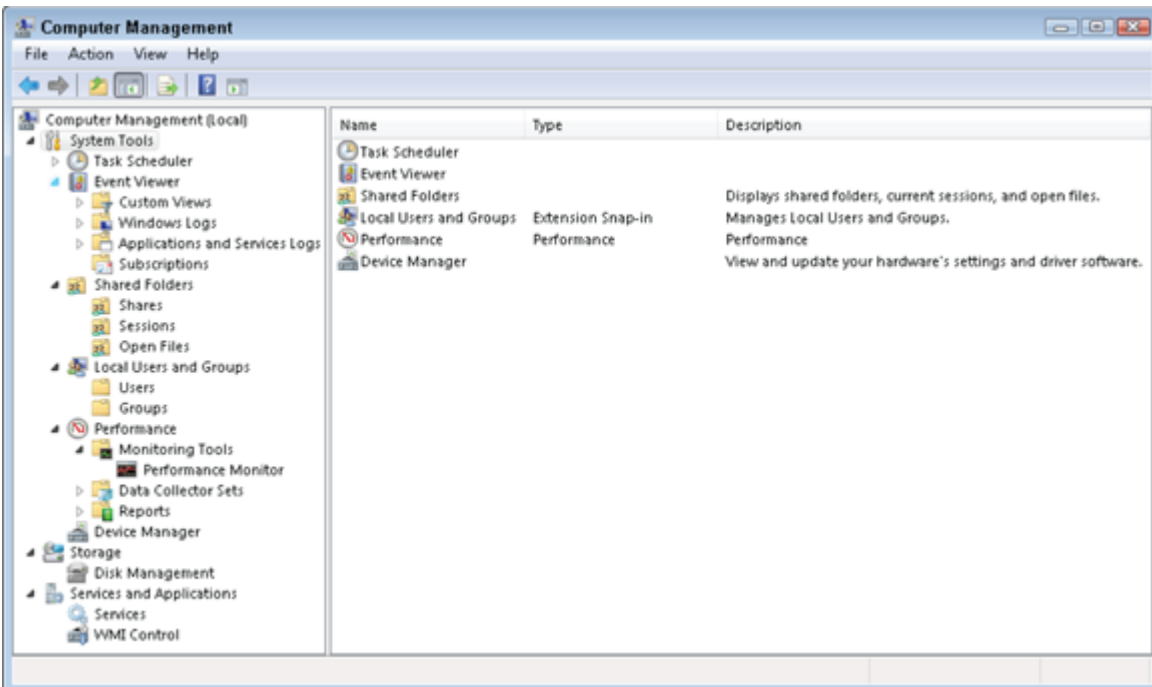
Module Name	Display Name	Driver Type	Link Date
=====	=====	=====	=====
1394ohci	1394 OHCI Compliant Ho	Kernel	9/11/2003 11:02:30 PM
3ware	3ware	Kernel	5/18/2015 6:28:03 PM
ACPI	Microsoft ACPI Driver	Kernel	
AcpiDev	ACPI Devices driver	Kernel	
acpiex	Microsoft ACPIEx Drive	Kernel	6/16/1975 10:07:59 PM
acpipagr	ACPI Processor Aggrega	Kernel	
AcpiPmi	ACPI Power Meter Drive	Kernel	7/26/1996 9:01:01 PM
acpitime	ACPI Wake Alarm Driver	Kernel	12/22/2010 5:58:01 AM
ADP80XX	ADP80XX	Kernel	4/9/2015 4:49:48 PM
AFD	Ancillary Function Dri	Kernel	

## *Computer Management*

Windows includes the Computer Management utility, shown in [Figure 4-17](#). Computer Management is actually more of a user interface to a number of other utilities than an actual utility. Computer Management is an MMC settings file that contains the following utilities or snap-ins:

- » **Event Viewer:** Shows the contents of event log files
- » **Shared Folders:** Shows the status of shared or published folders on the computer
- » **Local Users and Groups:** Manages the local account database
- » **Performance or Reliability and Performance:** Records system status and health based on measurable counters and generates alerts when the counters exceed threshold values
- » **Device Manager:** Displays hardware status and configuration information in a format that can be edited, unlike the System Information tool  
See the upcoming section, “[The System Information tool](#).”
- » **Disk Management:** Manages disk partitions

- » **Task Scheduler:** Manages and schedules tasks or applications to run automatically
- » **Services:** Manages system services (such as the Server and Workstation services) on the local computer
- » **Other administration utilities:** Other tools are included with this tool, including Telephony, WMI Control, Indexing Service, DNS, Internet Information Services, and Routing and Remote Access



**FIGURE 4-17:** Computer Management is your one-stop shop for system management utilities.



**TECHNICAL  
STUFF**

Computer Management is an MMC snap-in that acts as a container for other MMC snap-ins. The only offering or benefit over the individual tools is that you have to add only one snap-in to the MMC, rather than a whole series.

By putting all these utilities together in one location, system management is made substantially easier for most users.

In addition to using Computer Management to view and manage your computer, you can manage a remote computer:

1. **Right-click Computer Management (Local) at the top of the tree in the left-hand pane.**
2. **Choose Connect to Another Computer.**

This opens the Select Computer dialog box, from which you can type the name of another computer on the network.

3. **Click OK.**

After you are connected to that other computer, you can use all the management tools, with the exception of the Disk Defragmenter, which operates only on the local computer.



ON THE  
WEB

Lab 4-2 walks you through creating a custom Computer Management MMC. The labs can be downloaded from [www.dummies.com/go/aplusaio](http://www.dummies.com/go/aplusaio).

## *Component Services*

The first question you might ask about Component Services is what are they? Component Services are made up of Component Object Model (COM) components, COM+ applications, and the Distributed Transaction Coordinator (DTC) components. All these objects represent programming code that is registered on your computer. Programs on your computer use these components through system level calls to them.

The programming code used by these components is typically found in .dll files, and the components themselves are registered using `regsvr32.exe`. Once the .dll files containing these components are registered, you will find the object contained in Component Services MMC snap-in. The easiest way to access the Component Services management tool is to use `dcomcnfg.exe`. The main purpose of the Component Services tool is to adjust application launch and security

settings for the small programs that make up COM, COM+, and DTC objects.

### *services.msc*

The Services Administrative tool can be launched by running `services.msc`, where the `.msc` extension refers to a Microsoft Management Console (MMC)–saved console. The Services Administrative tool allows you to

- » See the services installed on your computer
- » Start, stop, and restart any service
- » Change parameters and startup settings for any services

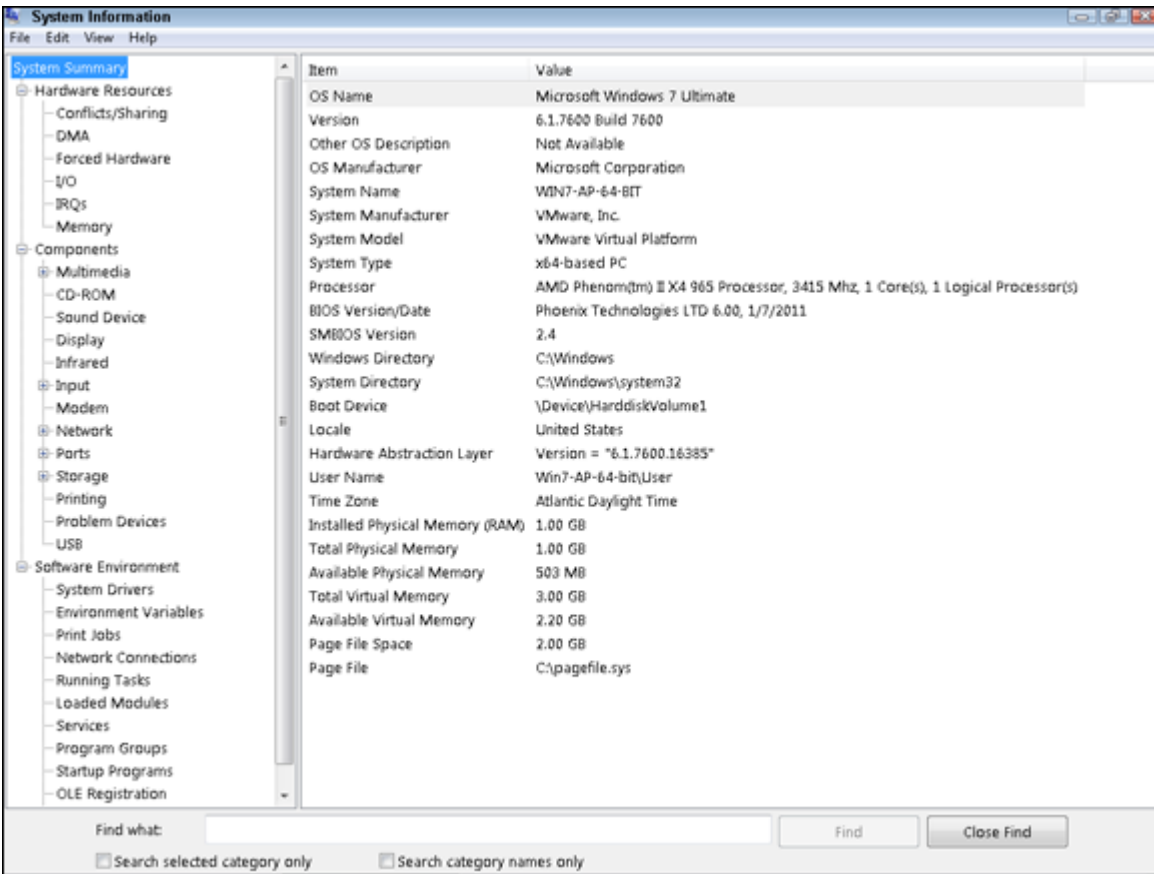
To find out more details about `services.msc`, review Book 6, [Chapter 3](#).

## *Getting a Handle on Diagnostic Utilities*

To figure out what is wrong with a faulty computer, you need to first find out everything it is doing, both right and wrong. The tools in the following sections are designed to provide you with information on a variety of areas of your computer.

### *The System Information tool*

The System Information tool (`msinfo32.exe`) is available in recent versions of Windows. This tool was designed to provide information about as many components in the OS as possible. [Figure 4-18](#) should give you a good feel for the type of information that is available within this tool. If it's part of the OS, the System Information tool can give you information about it.



**FIGURE 4-18:** The System Information tool provides information about your installation and hardware configuration.

To open the System Information tool, choose Start ⇒ All Programs ⇒ Accessories ⇒ System Tools ⇒ System Information. If you are using Windows 10, to open the System Information tool, choose Start ⇒ Windows Administrative Tools ⇒ System Information.

If you spend a few minutes investigating the data found in this tool, you will get a feel for the very detailed information it can provide. Very few areas of your system's hardware are not covered by this tool. It is well worth your time to get to know this tool to see what information it can gather.

If you want to save the current system information for archiving or to use as a baseline, choose File ⇒ Save to save the information into an NFO file, which can later be opened and viewed with the System Information tool.



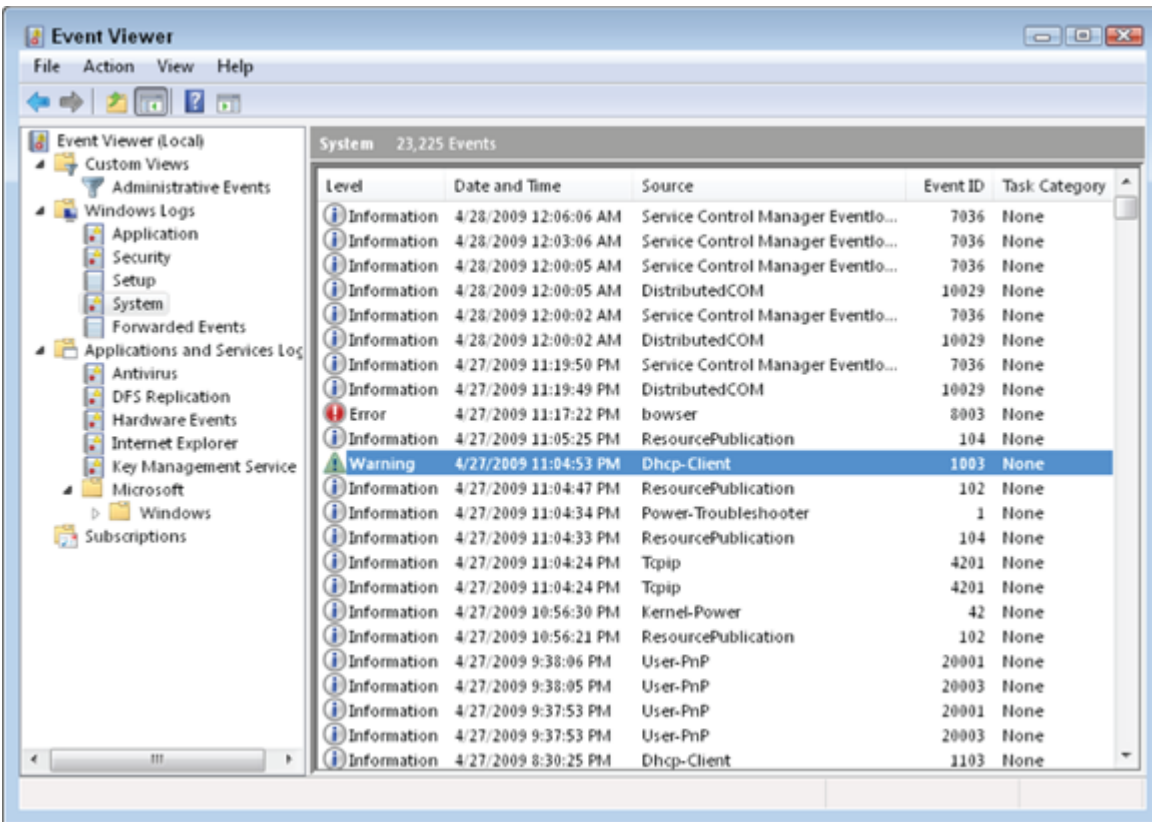
## *Event Viewer*

On some computers, you can check log files to look for errors with the system, applications, or hardware. Microsoft created a central logging and reporting tool that many components in the OS and many applications use. Any application can log events to the event logs or even create its own event logs to be viewed with the Event Viewer (the tool you use to view all this logged information) as well as configure log settings or clear the logs.

To view information, choose Start ⇒ Control Panel ⇒ System and Security ⇒ Administrative Tools ⇒ Event Viewer or run `eventvwr.msc`. On Windows 10, choose Start ⇒ Windows Administrative Tools ⇒ Event Viewer. The interface has the log files on the left of the screen and the log data on the right. There are five different log entry types and three default logs: System, Application, and Security.

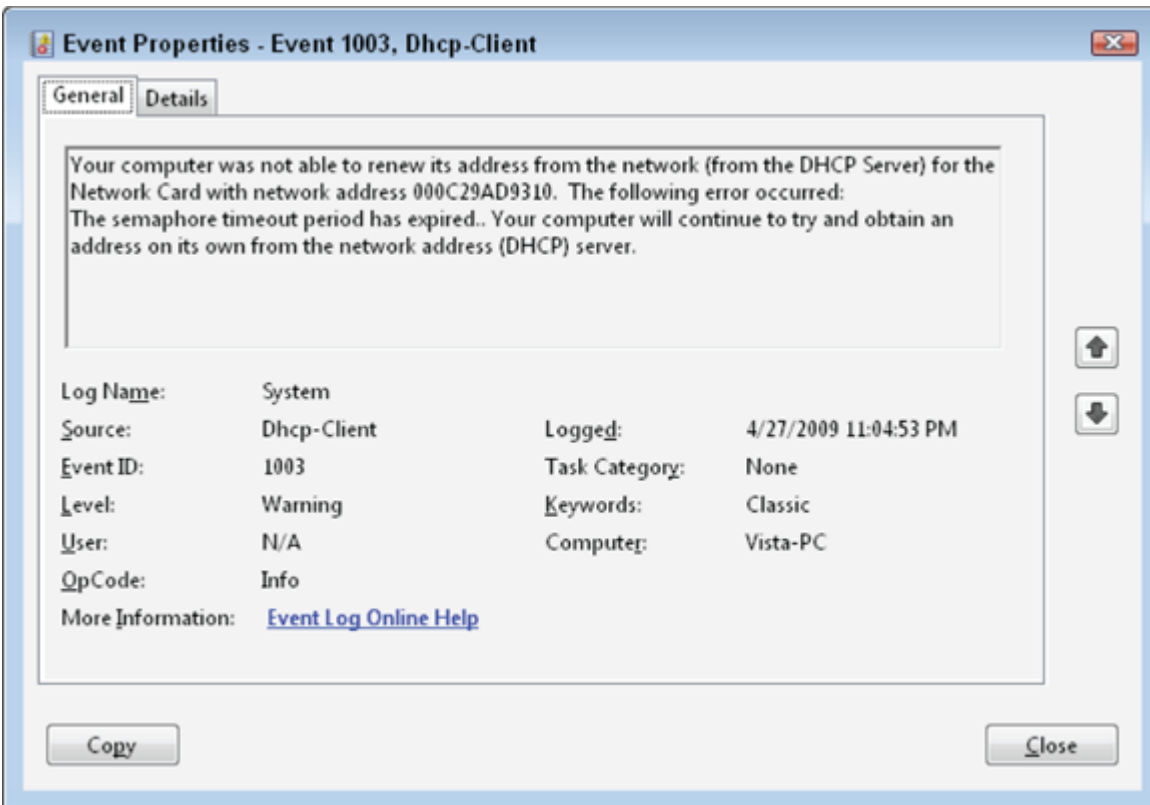
The Security log has two event types: either a lock or a key for Failures or Successes. The other two logs have three different entry types — Information, Warning, and Error — identifiable by symbol or color (blue, yellow, and red, respectively). To view log files on another computer, right-click Event Viewer (Local) in the left pane, and choose Connect to Another Computer from the shortcut menu. This opens the Select Computer dialog box, where you can type another computer name and then click OK.

[Figure 4-19](#) shows a typical System log. The Security log has audit information about your system if you have enabled auditing of system events or file system access. The System log records major system events, such as service failures, system startup or shutdown, and Stop events. The Application log records events from applications although you might find that some applications record their events in the System log, and some items thought of as system events are recorded in the Application log.



**FIGURE 4-19:** The System log has several types of messages telling you about major system events.

To see detailed information about the log entries, double-click any line item to bring up something that resembles [Figure 4-20](#), listing date and time, source (system area or application), type of event, event ID (the error code returned by the application), user (if related to a user account), computer (if related to a computer account), a text-based description of the error, and data (which might show raw data related to the event as hexadecimal and ASCII data).



**FIGURE 4-20:** The detailed information for an event gives you several relevant pieces of information.



**TIP** Read the Description section carefully because many developers put troubleshooting steps right into their error events.

To navigate to the next or previous events, use the arrows in the right side of the dialog box; to copy all event information to the Clipboard, use the Copy button. You can then directly paste this information into a document or email when reporting this event to other support people.

If you can't decipher the event message, you can find additional help at [www.eventid.net](http://www.eventid.net), which allows you to plug in the EventID and the source. Then you are able to view recorded events and descriptions of both the errors and the fixes. This site also contains links to the Microsoft Knowledge Base for articles related to the errors. To follow the links, you need to register on the EventID site, but because the site provides the Q article numbers (Microsoft's knowledge base has all articles number,

with a Q as the initial character in the filename), you can go directly to <http://support.microsoft.com> and locate the articles yourself.

When you right-click a log file, you have the option to save the event log as different types of text files or an EVTX file, which can be loaded back into Event Viewer, or to clear or empty the event log. The View submenu has options to allow you to find specific entries or filter the log file to show certain events. You can filter the log by any of the field values.

To change how long the log files are kept, right-click a log file and choose Properties. The default log file size in Windows is 20MB, but it can be set all the way up to 16EB (exabytes), and settings are available on what to do when the log reaches its maximum size. When it reaches its maximum size, you can overwrite events as needed, overwrite events older than a number of days (the default is seven days), or not clear the events at all (in which case, you stop logging new events).

In most cases, you should use Overwrite Events Older Than X Days and choose a number of days for which normal activity will not fill the log file. This system means that you can ignore the logging activity, but you will be notified when the log file fills up, and you can start your investigation into the activity that filled it prematurely. I typically leave this setting between 7 and 14 days, and make the size of the log file larger if necessary.

## ***System File Checker***

The System File Checker (`sfc.exe`) is part of the Windows File Protection interface and must be run by an Administrator. With the proliferation of applications and with software developers replacing stock Microsoft DLL files with custom versions, there is a real need for Windows File Protection and the System File Checker.

DLL (Dynamic Link Library) files contain compiled application code that is the same type of code that makes up an application. By saving this code as a DLL, the developer makes the code available to many applications so that it can be reused, reducing application development time. One dialog box found in a system DLL is the common Save As dialog box.

Windows keeps the cached copies of these files for your use when corruption occurs in the original files. Windows now takes active steps to prevent the deletion of core files, but in the past, you were able to easily illustrate this feature by deleting executables and DLLs and having them automatically replaced. The missing copy of the file will be replaced by the copy that was stored in the cache in

`%systemroot%\system32\dllcache` or `%systemroot%\WinSxS`. If the file was not in the cache, Windows will prompt you for the OS CD.

When you run the System File Checker, you have a choice of switches that you can use (depending on your version of Windows):

- » `/SCANNOW`: Immediately scans all files for incorrect versions, verifies the versions that are stored in the cache, and repairs any files it locates with problems
- » `/VERIFYONLY`: Only scans files and does not attempt to repair any issues it finds
- » `/SCANFILE`: Scans the integrity of a single file and repairs files it finds problems with
- » `/VERIFYFILE`: Verifies the file specified but does not repair the file
- » `/OFFBOOTDIR`: When performing offline repair (outside the current running copy of Windows), specifies the boot directory to use
- » `/OFFWINDIR`: When performing offline repair (outside the current running copy of Windows), specifies the Windows directory to use

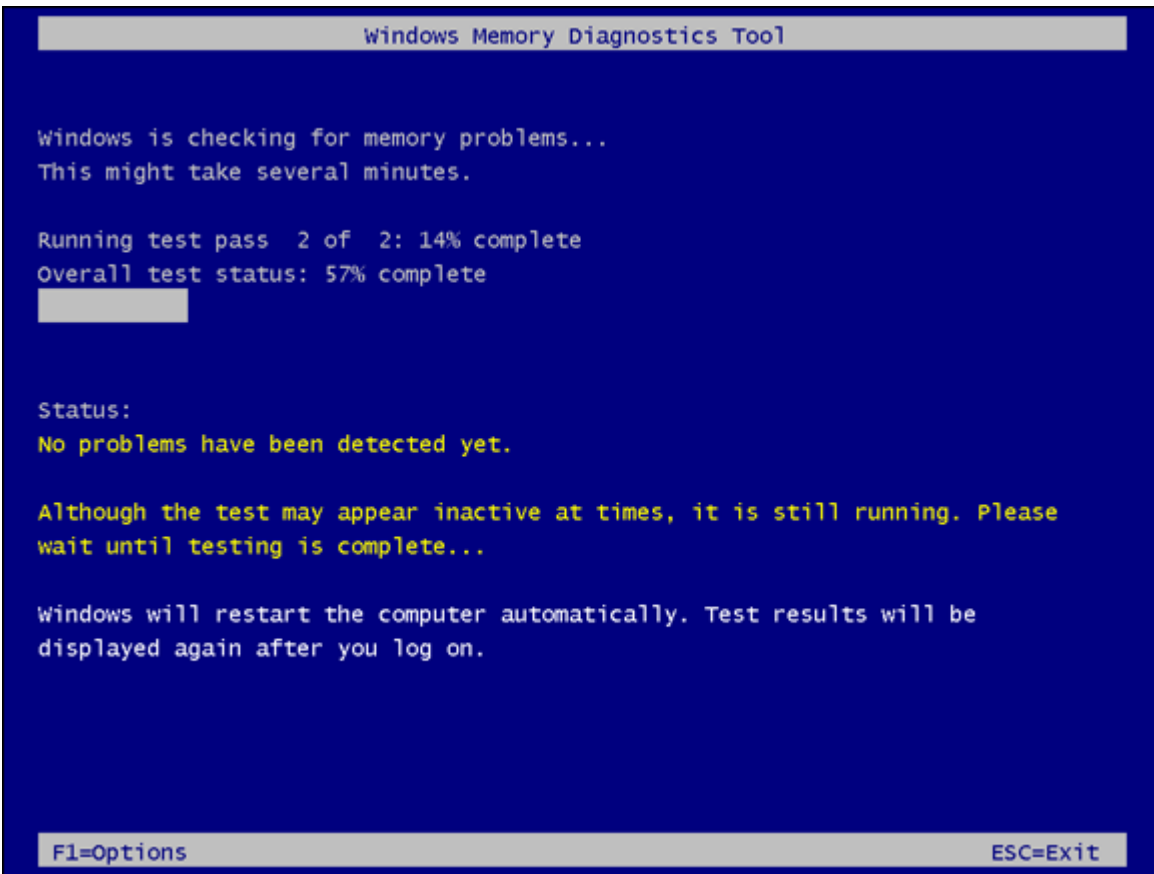
## *Windows Memory Diagnostics*

The Windows Memory Diagnostics tool does just what its name claims; it is a tool that can be used to test the memory on your computer. This tool is preinstalled on Windows. Now, for it to test the memory, it is best if that memory is not being used for anything else. To allow almost all system memory to be free for the running of the diagnostic tests, Windows uses a special boot process to only load the test tool. So, to start the test tool, run `%windir%\system32\MdSched.exe` or choose Start ⇒ Search, type

**Memory Diagnostics**, and select the tool when it is presented in the search results.

When you run Windows Memory Diagnostics, it will present you with a simple window asking you to either restart now or to run the tool on your next start of Windows. The choice is yours. When it reboots, it will automatically launch the test tool.

The tool will automatically start running the default tests on memory, as seen in [Figure 4-21](#). If you would like to change the settings, follow the onscreen commands and press F1. This will bring you to the configuration screen, where you can change three settings. The first is the Test Mix, where you can choose from Basic, Standard (default), or Extended. The test mix determines the exact tests that will be executed against the memory on the computer. The second option you can adjust is whether the system cache memory will be used for tests. A default setting exists for cache use on each test, but you can force it to be on or off for all tests. The third setting is how many times you want to run the tests, which the test calls passes. Most major memory errors will appear on the first pass, while others are sporadic; in the latter case, it may take several passes to see the error. The pass count can be set up to 99 passes.



**FIGURE 4-21:** Windows Memory Diagnostics is a special command screen that operates on a special reboot of Windows.

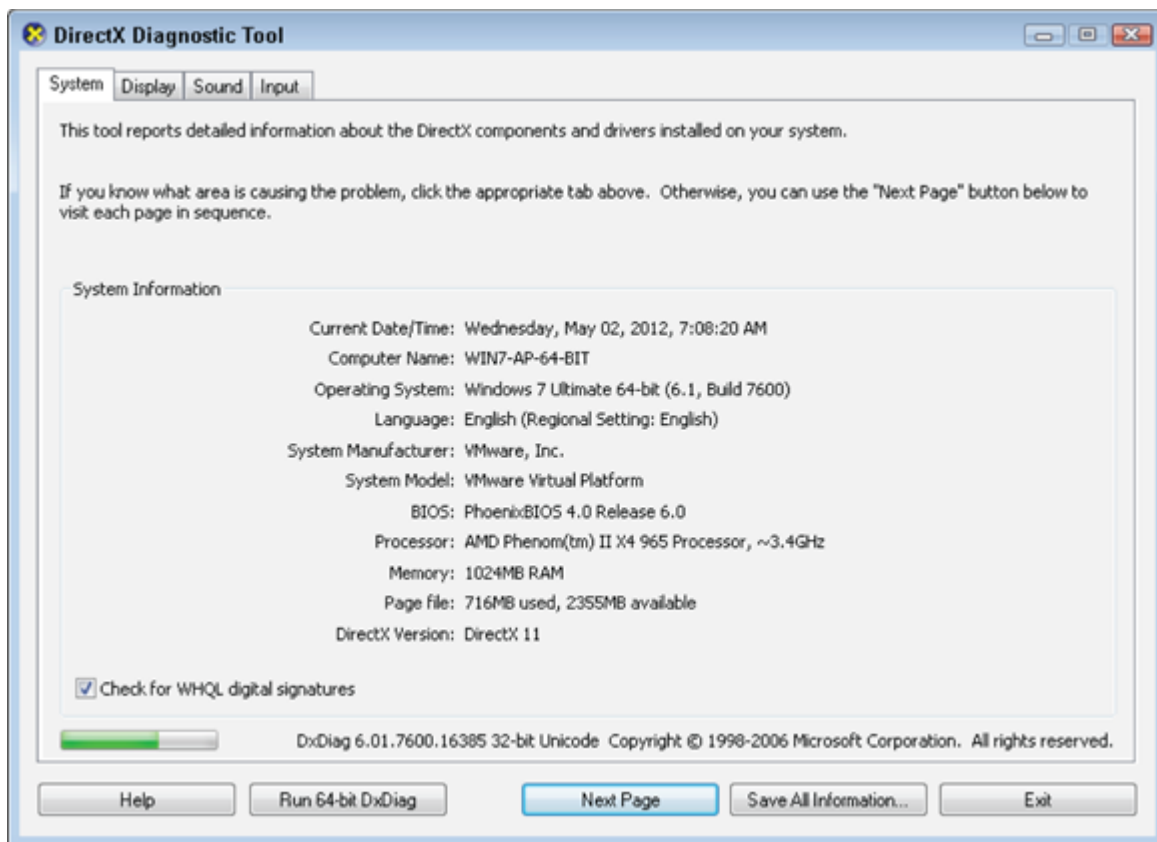
If Windows Memory Diagnostics reports any errors, it is likely that you have a hardware error related to memory on your computer, and you will need to replace the defective memory. See Book 2, [Chapter 3](#) to review the process of replacing memory in a computer.

### *DirectX Diagnostic Tool*

The last diagnostic tool that you see in this chapter is the DirectX Diagnostic Tool, or `dxdiag.exe`. This tool will evaluate the high-performance audio and video systems on your computer. Some applications, primarily games, make use of the DirectX drivers on your computer to assist in rendering high-speed graphics.

The main purpose of `dxdiag.exe` is to evaluate these systems through an easy-to-view screen, as shown in [Figure 4-22](#). To launch `dxdiag.exe`, choose Start ⇒ type **dxdiag.exe**, and select `dxdiag.exe` from the results

list. When the tool launches, it will first ask you whether you would like to test the drivers to ensure that the drivers are all signed and tested by the Windows Hardware Qualifying Labs. Upon opening the main tool, it will automatically start testing the drivers on the system. You will see detailed information about the drivers in use on the system from the System, Display, Sound, and Input tabs.



**FIGURE 4-22:** DirectX Diagnostics gives you a quick snapshot of the DirectX driver status on your computer.

## *Miscellaneous Utilities*

A number of miscellaneous utilities are also available within Windows. The following sections take a look at some of them.

### *Task Scheduler*

The system Task Scheduler service is responsible for running scheduled tasks. This service (like all services) runs in the background — and in



this case, making sure that your tasks are performed at the times you planned.

Your interface to this service is found via Start ⇒ All Programs ⇒ Accessories ⇒ System Tools ⇒ Task Scheduler, which opens the Task Scheduler window. If you are using Windows 10, choose Start ⇒ Windows Administrative Tools ⇒ Task Scheduler.

To schedule a task, follow these steps:

- 1. Click Create Basic Task.**
- 2. In the Create Basic Task Wizard that opens, type a name and description for the task, and then click Next to continue.**
- 3. Select the scheduled interval for the task, which includes**

- Daily
- Weekly
- Monthly
- One Time Only
- When My Computer Starts
- When I Log On
- When a specific event is logged

- 4. Click Next.**

Depending on your scheduled interval, you will be presented with different scheduling times.

- 5. Specify the exact times you want the task to run and then click Next.**
- 6. Select the action you want the task to perform and then click Next.**

The main action is Start a Program, while two deprecated options are Send an Email and Display a Message.

- 7. Browse to a program or script you want the task to run (you can provide arguments as a directory for it to start in) and then click**

## Next.

You are now on the last screen of the wizard. You can choose the check box to Open the Properties Dialog When I Click Finish to view the properties for the task, which include the settings already discussed for this wizard, as well as these settings which will be on the Conditions and Settings tabs:

- Do not run the task if you have a laptop running on batteries.
- Maximum duration for the task to run.
- Run the task only if the computer is idle, and stop the job when the computer is no longer idle.

**8. If you do not want to view these settings, just click Finish; otherwise, select the Open the Properties Dialog When I Click Finish check box, and then click Finish.**

When you exit the wizard, you will see the new task in the Task Scheduler's Task Scheduler Library folder. To see the properties for any task, select the task and right-click Properties or view the properties at the bottom of the window. From the properties window of the task, you can adjust the general properties, triggers, actions, conditions, and settings. The history of the command execution will be shown on the History tab. If you do not want to wait for the schedule but rather have the task run immediately, select the task, right-click it, and choose Run from the shortcut menu. You will see the status of the job change to Running. The other information shown in the Scheduled Tasks folder includes

- » When the task is scheduled to run next
- » When the task last ran
- » The status or what error code was returned the last time the task was run



**TIP**

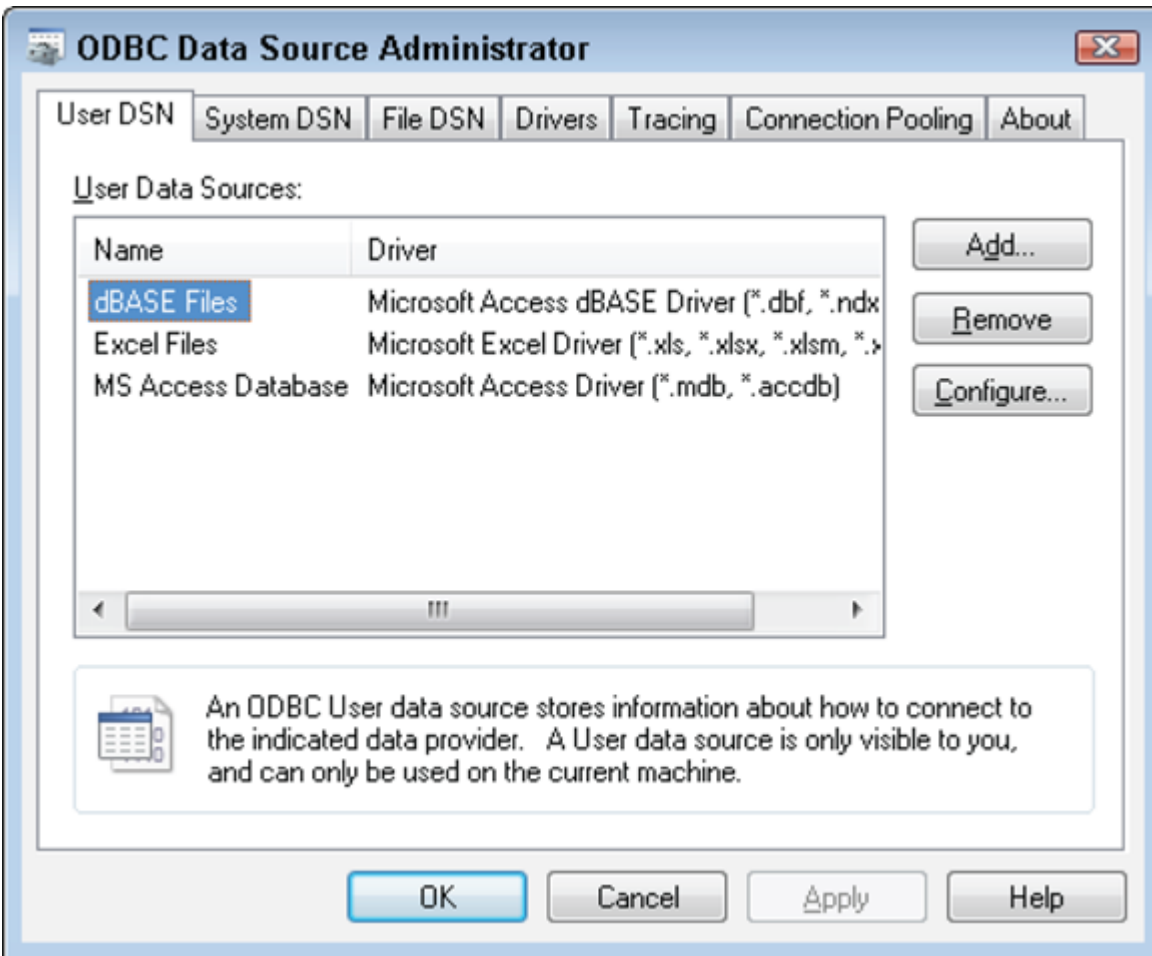
0x0 is the standard code for a successful execution.

## *Data Sources*

The ODBC Data Sources tool is found in the Administrative Tools folder is a configuration tool for data sources. Data sources provide you with the ability to store or retrieve information from a database using a common interface. Databases are often used by troubleshooting and logging tools to store data, but you may also need to troubleshoot database connections for other applications. The configuration information found in this section should help you in identifying data source configuration issues.

The main user interface for these database connections is the Data Sources (ODBC) Administrative Tool, which can be launched by choosing Start ⇒ Control Panel ⇒ System and Security ⇒ Administrative Tools ⇒ Data Sources (ODBC) or by running `odbcad32.exe`. If you are using Windows 10, choose Start ⇒ Windows Administrative Tools ⇒ ODBC Data Sources (32-bit) or ODBC Data Sources (64-bit). When Data Sources opens, you will see the seven tabs shown in [Figure 4-23](#). The main tabs that you will focus on are

- » **User DSN (Data Source Name):** Used to manage user-based database connections. Connections created on this tab will only be available to the current user.
- » **System DSN:** Used to manage system-based database connections. Connections created on this tab will be available to all users of the computer.
- » **File DSN:** Used to manage file-based database connections. The files created by this process can be shared by any users who have the required database drivers installed on their computers.



**FIGURE 4-23:** Data Sources allows you to manage database connections.

The process to create a new DSN is fairly straightforward, and this process will show you how to create a new System DSN used to connect to a Microsoft SQL server:

1. **Open the Data Sources (ODBC) Tool by choosing Start ⇒ Control Panel ⇒ System and Security ⇒ Administrative Tools ⇒ Data Sources (ODBC); if you are using Windows 10, choose Start ⇒ Windows Administrative Tools ⇒ ODBC Data Sources (32-bit) or ODBC Data Sources (64-bit).**

The ODBC Data Source Administrator opens.

2. **Select the System DSN tab.**
3. **Click the Add button to create a new data source.**

The Create New Data Source window opens.

**4. Select SQL Server and click the Finish button.**

The Create New Data Source to SQL Server window opens.

**5. Type a descriptive name for the new data source and a description, and specify the server to which you want to connect. Then click the Next button.**

**6. Specify the type of authentication you would like to use; then choose Next.**

You can use your current Windows logon credentials or credentials specific to the SQL server. You can override the default connection settings by clicking the Client Configuration button. Finally, you can make an initial connection to the SQL server to get server-specific information.

**7. You can change to a different default database, which is otherwise assigned by the server, or manage other connection settings to the database.**

The defaults are general settings, which work well for most applications, but you will want to check your application documentation to see if specific settings are required. Click Next to continue.

**8. Select the needed logging and other advanced connection settings if necessary; then click Finish.**

Again, the defaults are likely sufficient, unless application-specific documentation suggests otherwise.

This displays a summary page for the wizard. The summary page allows you to verify the settings that you are using, as well as allows you to test the connection to the data source.

**9. Click the Test Data Source button to make a test connection to the server. When you are happy with the connection, click OK to complete the wizard.**

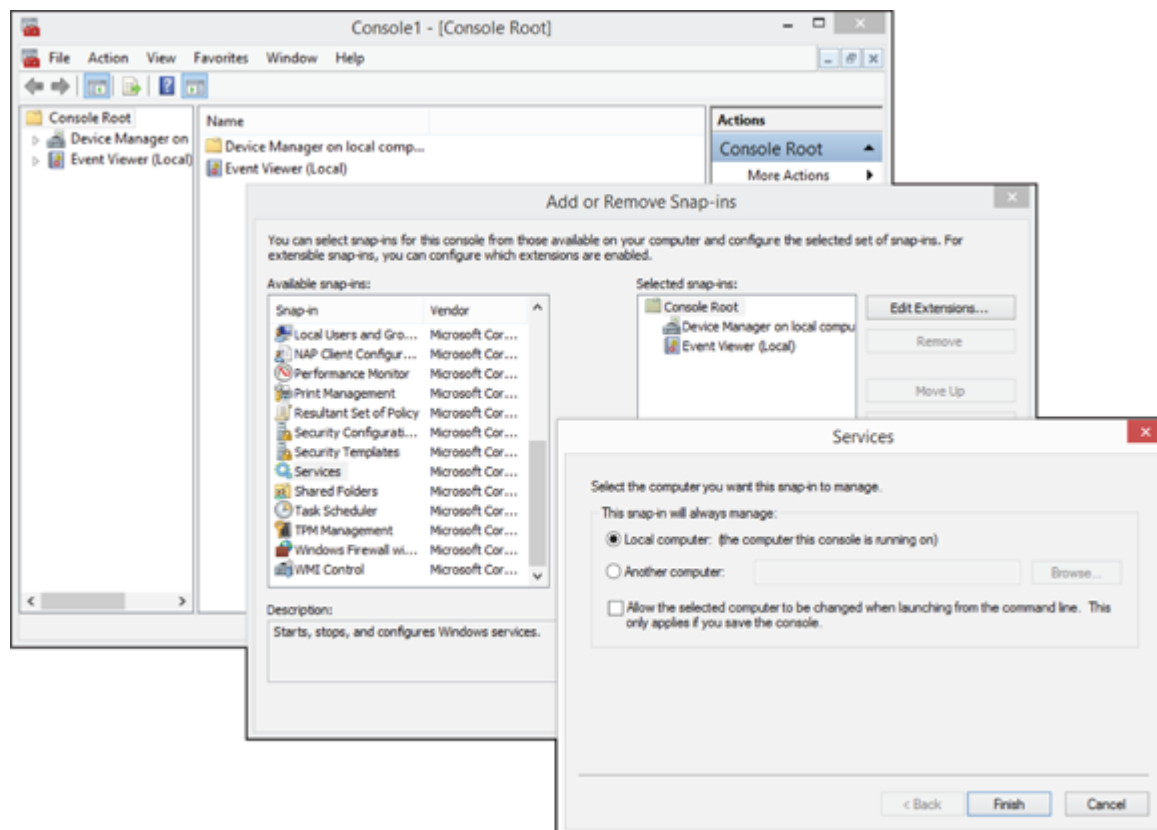
With the data source creation completed, you should see the new connection listed on the System DSN tab.

## *Microsoft Management Console*

The Microsoft Management Console (MMC) is the main management interface for all Microsoft management tools. Prior to the implementation of the MMC, you used to have a separate tool for each component you wanted to manage. With the MMC, you now have a common interface for all management tools. Each management tool is now a snap-in to the main interface.

To launch a blank console for the MMC, choose start and type **mmc.exe**. Once the blank console is launched, you can load snap-ins by using the following steps:

1. **Open the MMC by choosing Start and then typing mmc.exe.**  
A blank MMC console opens.
2. **Choose File ⇒ Add/Remove Snap-in.**
3. **From the Add or Remove Snap-ins dialog box, select the snap-in you would like and click the Add button.**  
When you add some snap-ins, you will be prompted to add them to manage the local computer or a remote computer, as shown in [Figure 4-24](#).
4. **Once you have installed or removed all the snap-ins you want to, click the OK button.**



**FIGURE 4-24:** When adding snap-ins to MMC, you can often target another computer.

If you think that you will need to use the same combination of snap-ins in the future, choose File ⇒ Save or File ⇒ Save As to save a copy of the current console. MMC saved consoles have an extension of `.msc`.



**ON THE WEB**

Lab 4-2 walks you through the process of creating a custom Computer Management MMC. Lab 4-2 can be downloaded from the companion website at [www.dummies.com/go/aplusaio](http://www.dummies.com/go/aplusaio).

## *Microsoft Terminal Services Client*

The Microsoft Terminal Services Client (`mstsc.exe`) might not always be thought of as a troubleshooting tool, but when you are miles away from the computer for which you need to perform troubleshooting, this tool will be part of your arsenal. With the MSTSC, you will be able to remotely connect the computer and access most functions as if you were sitting in

front of the computer. This tool is also called Remote Desktop Connection, which is covered in Book 5, [Chapter 2](#).

## *Notepad*

Another tool that is not often considered to be a diagnostic tool is `notepad.exe`. When working with configurations and logs on a Windows computer, it is not uncommon to encounter text files. In almost every situation when you encounter a text file, the best program to use is `notepad.exe`.

## *Explorer*

Explorer is the Windows File Explorer and is used to locate files on your computer. As with `mstsc.exe` and `notepad.exe`, these tools are not truly diagnostic tools, but rather tools that you will use to work with files on your computer. File Explorer will be used to move files, recover files from the Volume Shadow-Copy Service (VSS), or back up files.

# *Getting an A+*

This chapter examines several Windows-based utilities. You find out about the following:

- » Disk maintenance programs, such as `defrag`, and `chkdsk`, are used to improve performance and reliability of the disk subsystem.
- » Creating and managing disk partitions with Disk Management.
- » Configuration utilities, such as the System Configuration utility, System Information tool, Registry editors, Registry scanners, Device Manager, and the Computer Management Console, are used to view or change Windows configuration settings.
- » `wordpad.exe` or `notepad.exe` can be used to create or modify text files.
- » `expand.exe` can be used to decompress Windows source files.

## *Prep Test*



- 1. You have stopped by a user's desk to find that he has been searching his hard drive for the program `defrag.exe`. To test his knowledge, you ask him, “`defrag.exe` does what for your computer?”**

  - (A) Rearranges memory so that access to it is improved
  - (B) Removes dust and fragments from your computer
  - (C) Rearranges data on your disk drive so that access to it is improved
  - (D) Recovers files that have been corrupted
  
- 2. Based on issues you have described in conversation, your co-worker has suggested that you run the `chkdsk.exe` program on your problem computer. `chkdsk.exe` can do which of the following?**

  - (A) Rearrange data on your drive so that disk access is faster.
  - (B) Consolidate free space on your hard drive.
  - (C) Correct problems with file storage on your hard drive.
  - (D) Change the partition table of the drive from FAT16 to FAT32.
  
- 3. You and a co-worker have a disagreement related to the proper name of the Registry modification tools in use on Windows computers. What programs can be used to edit the Registry on a Windows computer?**

  - (A) `registry.exe`
  - (B) `cfgedit.exe`
  - (C) `regedt32.exe`
  - (D) `regedit.exe`
  
- 4. You need to send a copy of specific registry keys to a customer, who will import them into her computer. What command is used to export a section of your Registry while using `regedit.exe`?**

  - (A) File ⇒ Export Registry File
  - (B) File ⇒ Extract to Recovery File
  - (C) Export ⇒ Set Restore Options

(D) File ⇒ Backup Key

**5. After exporting a group of Registry settings to a .reg file, you need to make some changes to the settings. What tool should you use to change an exported Registry file?**

- (A) sysedit.exe
- (B) regedit.exe
- (C) notepad.exe
- (D) Microsoft Word

**6. You are concerned that some of your Registry files on your computer may be missing. Which files on your hard drive make up the Windows Registry?**

- (A) system.dat and registry.dat
- (B) user.dat and system.dat
- (C) user.dat and hardware.dat
- (D) system, sam, security, and ntuser.dat

**7. You have a script that needs to run every Monday at 9:00 a.m. What tool can you use to make this script run at that interval?**

- (A) Remote Desktop Connection
- (B) Registry Editor
- (C) Explorer
- (D) Task Scheduler

**8. You need to find out which memory addresses are being used by a driver. What tool will tell you what you need to know?**

- (A) memedit.exe
- (B) System Resource Meter
- (C) Device Manager
- (D) System Driver Checker

**9. You are setting up a storage space for your server and you want to ensure that you only allocate the minimum amount of space required to hold the data on disks. What option would you need to specify when configuring the storage space?**

- (A) Triple Mirror
- (B) Mirror
- (C) Thin
- (D) Full

## *Answers*

1. **C.** `defrag.exe` rearranges data on your disk so that access to files is faster. By allowing your disk to perform reads of data in contiguous blocks, it takes less time to read files. See “[diskpart.exe and Disk Management](#).”
2. **C.** `chkdsk.exe` fixes minor problems with files that are stored on your hard drive and can also test and verify the clusters on your drive. Review “[chkdsk.exe \(Check Disk\)](#).”
3. **D.** `regedit.exe` is the editor for Windows computers. If you run `regedt32.exe`, you will actually open `regedit.exe`, which you can verify in the Task Manager. Peruse “[regedit.exe](#).”
4. **A.** Export Registry File from the Registry menu will export a section of your Registry. Take a look at “[regedit.exe](#).”
5. **C.** Registry import files must be straight text. WordPad and many other programs that edit text files add different characters to handle carriage returns and line feeds. This can create files that will not be imported through `regedit.exe`. Peek at “[regedit.exe](#).”
6. **D.** `system`, `sam`, `security`, and `ntuser.dat`, in addition to software, are the files that make up the Registry. All the files are found in `<%systemroot%>\system32\config`, with the exception of `ntuser.dat`, which is found in each user’s profile directory. Look over “[regedit.exe](#).”

7. **D.** The Task Scheduler allows you to schedule processes to run at specific times or when a computer is idle. *Study “[Task Scheduler](#).”*
8. **C.** Device Manager will tell you what resources are being used by which devices. *Refer to “[Device Manager](#).”*
9. **C.** Thin provisioned disks set the actual disk size to grow as data is written to disk, which minimizes the size of the disk. *Review “[Working with Disk Management](#).”*

# Chapter 5

## Scripting within the Operating System

---

### IN THIS CHAPTER

- » Understanding basic programming techniques
  - » Introducing batch files and VBScript
  - » Introducing Windows PowerShell
  - » Looking at Shell Script and Python Script Basics
  - » Introducing JavaScript Syntax
- 

As an A+ Certified Professional, you will want to use the full range of tools available to you. This chapter introduces you to the world of scripting, which can be used in conjunction with other content in this book to set up automation tasks to make your job easier. A script can migrate files around your network, back up settings, or create a report related to changed settings. Basic knowledge of scripting is helpful for all A+ certified technicians, not only for the exams, but also to help automate common administration tasks on the job.

The scripting or automation languages discussed in this chapter are as follows:

- » Batch files and VBScript
- » PowerShell
- » Shell script and Python script
- » JavaScript

When taking a look at these options, you will see how to use basic program flow and control structures, which include parameters, logic

controls, loops, functions, and subroutines. When you see the remaining languages, you will draw on the knowledge introduced in earlier sections of the chapter. Although the language and syntax may change, the concepts remain consistent for any programming language.

## *Creating Your Files*

Regardless of the type of scripting language you decide to use, you will need to edit text files to create your scripts. You can use any text editor to create a script file. For example, on a Windows system, the most consistent program to use is Notepad. Many administrators will download a third-party text editor because it offers many features such as syntax coloring, syntax highlighting, indentation, and line numbering.

Following are some common file types you will create as scripts:

- » **.bat:** A batch file that was common in Microsoft operating systems for many years. These files contained DOS or Windows command prompt commands.
- » **.vbs:** A Visual Basic script file can contain VB script code that is similar to the Visual Basic language, but not as powerful. These files were used to automate the administration of a Windows system.
- » **.ps1:** A PowerShell script file. PowerShell is the newest scripting environment for Windows systems and is a powerful tool to automate administrative tasks.
- » **.sh:** This is a shell script file used on Unix or Linux systems to automate tasks.
- » **.py:** A Python script file used to automate administration of a system. Python can be used on Windows, Mac, or Linux systems. You must have a Python interpreter installed in order to execute Python scripts on these systems.
- » **.js:** A JavaScript file typically used by web developers to execute script on a web page.

To start a script file, you need a place to put the commands you want to execute. To do this, open the text editor of your choice, make a new text file, and save it with an appropriate extension (.bat, .ps1, or .vbs).



**TIP** If you're using a Windows-based editor (such as Notepad) and the operating system option of Hide File Extensions for Known File Types is enabled, you must enclose your filename in quotation marks when saving it.

If you want file extensions to show in Windows 7, use the following steps:

1. **Open Computer.**
2. **Choose Tools ⇒ Folder Options.**
3. **Click the View tab.**
4. **Deselect (to show) the Hide File Extensions for Known File Types check box.**
5. **Click OK.**

For newer operating systems such as Windows 10, use these steps to view file extensions:

1. **Choose File Explorer from the task bar.**
2. **Choose View and then enable File name extensions.**

With your file open in the text editor, you can now type any commands you want, but remember to put only one command per line in your file. For a batch file, you can use this file to create, copy, or delete files, or anything else that you could do from the command prompt.

After you create a file, you can execute it directly if it is a batch file by typing the path to the file and the filename at the Start ⇒ Run command or at a command prompt. VBScript files and PowerShell files may take a little more to get going.

When working with PowerShell, Microsoft provides a tool that towers over Notepad — `powershell_ise.exe`, the PowerShell Integrated Scripting Environment (ISE). Either Notepad or the PowerShell ISE can be used to create PowerShell scripts. Tabs at the top of the editor allow you to have multiple files open at once, and the multiple panes allow you to edit the script, execute it, and see the output without needing to move between applications. In addition, because the ISE knows PowerShell, it performs syntax coloring, which makes it easier to read and follow your code.

## *Going Back to Basics with Batch Files*



**WARNING** I strongly recommend doing testing with the batch file on a test computer. I have seen people create batch files with improperly formatted `rmdir` commands, which then deleted many more files and directories than expected. If you use commands that format partitions, remove files, or delete disk partitions, note that poorly structured commands might result in you being required to re-install the operating system on your computer. The commands suggested in this section are not dangerous.

### *Getting your directions*

Many people want to be able save the output of their commands — or, more rarely, answer questions or provide input for a command. There are a few ways to do this, and [Table 5-1](#) summarizes the differences among the options. All options require that your program is generating output going to `stdout` (standard output) or accepting input from `stdin` (standard input).

---

---

#### **TABLE 5-1 Redirection Symbols**



---

**Symbol Function**

---

<	Sends the contents of a file listed on the right into the command on the left. This is useful when you want to provide an answer to a question that a command will prompt for (for example, when the <code>format</code> command prompts for confirmation). By creating a one-character text file with just <code>y</code> and a return or enter, you can pass a yes into the <code>format</code> command.
>	By specifying a command on the left and a text file or <code>nul</code> on the right, you can prevent output of a command from going to the screen. Instead, output is passed to the file listed on the right side. If the file exists, it will be overwritten. This is extremely useful if you want to log the results of certain statements.
>>	Similar to the <code>&gt;</code> symbol except that the output is appended to the destination file if it already exists. If the file does not exist, it will be created.
	The pipe “pipes,” or directs, the output of the file that is listed on the right side into (as input) the command listed on the left. This may allow you to bypass the creation of a text file.

---

---

`stdout` and `stdin` are interfaces or objects that C programmers use almost exclusively when requiring data input and output for command line programs. As a programmer, I can write an application that sends its output to an interface called `stdout`, and then I let the operating system deal with where that actually is: It might be a teletype terminal, printer, monitor, or text file. For all versions of Windows, data sent to `stdout` will be displayed in a command prompt window.

## ***Working with parameters or starting arguments***

You can get a lot more mileage from your batch files if you pass and use arguments with them. An *argument* is a piece of data passed to the batch file or command when typing the command, such as

```
copy C:\this.txt C:\that.txt
```

which has two arguments: `C:\this.txt` and `C:\that.txt`. You can use ten arguments with a batch file. This really drops off to nine because the first argument is `%0`, and that represents the name of the running batch file. `%1` through `%9` can be used as arguments for your batch file. If you have a batch file that copies files from one directory to another, you can make your batch file more reusable by working with arguments. Here is an example of this concept:

Old batch file — `StaticCopy.bat`:

```
xcopy c:\dos\*. * c:\dosback
```

This file could be made more generic with these modifications:

New batch file — `DynamicCopy.bat`:

```
xcopy %1 %2
```

This new batch file would be run by using

```
dynamiccopy c:\dos\*. * c:\dosback
```

It's true that you are typing more to achieve the same result. But you have to consider that this line could be in a much larger batch file, which could use the two parameters (`%1` and `%2`) in many different ways. This could actually save you a lot of typing when creating and editing your batch file because the parameters can be used rather than hard coding the paths or parameters.

This system works fine until you find yourself in a position in which you need more than nine parameters passed to your batch file. However, if you plan the order in which you use your parameters, you can actually support many more than nine. This is done with the `shift` command. Each time you use `shift` in your batch file, all parameters that are passed to your batch file are shifted over one position. For example, `%2` becomes `%1`, `%3` becomes `%2`, and so on.

## *Making batch files make decisions*

So far, you have seen some ways to make your batch file more generic. Now, I show you how to make it think for itself — or at least think for you. There are two ways to get your batch file to make some decisions although after you read this section, you might argue that there is only one way, seeing as how both ways make use of batch file labels.

### *If statement*

First, the `if` and `:label` statements introduce simple program flow logic. For example, if you know that you need two parameters passed to your batch file for it to work properly, you can use something like [Listing 5-1](#) in your batch file:

## **LISTING 5-1 Passing Two Parameters to a Batch File**

---

```
if not !%2==! goto correct

:Instructions
echo.
echo Please provided two parameters. The first is the
echo source directory, and the second is the destination.
echo.
goto end

:correct
xcopy %1 %2
goto end

:end
```

When working with the `if` statement, you evaluate whether two options are the same or whether a condition is true. In this case, you are testing for two items being equal. To do this, you need two items because you cannot test equality with only one item. In this example, you want to see whether the second parameter is blank, so you use `%2`, which represents the second parameter. However, you cannot use `if not %2==` because that would evaluate `%2` to nothing, and you need something on the other side of the equation. This gets worse if the second parameter was not passed to the batch file because `%2` will not exist, and you are then asking whether nothing equates to nothing. The `if` statement cannot handle evaluating nothing in an equation.

To make sure there is something to evaluate on both sides of the equation — and not change the results — you need to add a character to both sides of the equation. In this example, I chose to use the exclamation mark. You should also take note of the use of the word `not` to reverse the results of the test.

### ***Environment variables***

Some other items that the `if` statement can test for includes OS environment variables and whether files and directories exist. To test an

environment variable for a specific value, you use a command like this one that checks the name of the computer that is running the batch file:

```
if !%COMPUTERNAME%==EDSPC goto instructions
```

To test whether a file exists, you use something like

```
if exist c:\autoexec.bat goto Instructions
```

If you want to know whether a directory exists, you can test for `nul`, which only exists for your test if a directory is there:

```
if exist c:\windows\nul goto Instructions
```

The full example also shows you how to work with labels and the `goto` statement. The `goto` statement uses only the first eight characters of the label, so try to keep label names unique. The `goto` statement requires a destination in the batch file to be sent to, and that is where the labels come in. Although `end` is a label that is meaningful to you, it is just another label to the batch file.



**REMEMBER** If you use a `goto` in your batch, you must have a matching label, or you will get errors, and your batch file will not work.

### *Choice statement*

The last method of controlling the flow of your batch file is using the `choice` statement. The `choice` statement allows you to pause your MS-DOS or Windows batch file to wait for input. Input to the `choice` statement is a single character. [Listing 5-2](#) shows an example of how to use the choice statement:

## **LISTING 5-2 Using a Choice Statement**

---

```
@echo off
choice /c:ynm /M "You choose"
if errorlevel == 3 goto m
if errorlevel == 2 goto n
if errorlevel == 1 goto y
goto end
```

```

:y
echo You chose Yes.
goto end

:n
echo You chose No.
goto end

:m
echo You chose Maybe.
goto end

:end

```

The `choice` statement uses the list of parameters after the `/c:` to listen to input. One of those choices must be provided. The `choice` statement will actually ignore any other input and wait for one of those choices.

Also, take note of how to handle the input afterward. Each choice is assigned a number, based on its order: `Y` = 1, `N` = 2, and `M` = 3. The `if` statement should actually be read as, “If the error level is greater than or equal to `x`, go to label.”



**TIP** Because of how the computer handles `if` statements, always test the `errorlevel` from the highest to the lowest. If you test the values in the wrong order and start your evaluation with `if errorlevel = 1 goto y`, everything will satisfy this test because all possible values are greater than or equal to 1.



**REMEMBER** The `if` and `choice` statements add many options to the design of your batch files; they can help you make batch files that are flexible and comprehensive.

## *Looping*

I hate having to repeat myself, and if you feel the same way, loops are for you. Loops can be used inside or outside batch files with only a small modification. The loop is a `for` loop and requires a list of values that are assigned to a variable and a statement that uses that variable. The variable is assigned with a preceding `%` character outside a batch file, and two `%` characters when used within a batch file. Here is an example of a loop at the command prompt:

```
echo off
for %x in (hello world) do echo %x
```

The output of the previous loop would be

```
hello
world
```

If done in a batch file, the loop would look like this:

```
echo off
for %%x in (hello world) do echo %%x
```



**REMEMBER** Loops may cut down your work when you have several repetitive lines in your batch file.

## *Locating a command*

When you type a command at a command prompt, in a batch file, or at the Run command, your computer follows a set of steps to locate the command:

1. The computer checks the current directory for the command.
2. If the command is not found in the current directory, the computer checks all directories listed in the Path environment variable.

If the command is not located — possibly because you misspelled it — you see the following message:

```
Bad command or file name
```

If you are using Windows Vista or newer, then the message will look like the following:

```
'notaprogram.exe' is not recognized as an internal or external command,  
operable program or batch file.
```

If you see this message, check the spelling of the command and try again.

The path variable can be set in the `autoexec.bat` file for all Microsoft OSes. It is the only environment variable that can be set without using the `set` command. To set the path variable, you can use either

```
set path = c:\windows;c:\windows\system
```

or

```
path = c:\windows;c:\windows\system
```

The only advantage to the latter is that it uses four fewer keystrokes. If both `c:\windows` and `c:\windows\system` are in the path, they will be checked when a command that is typed is not in the current directory.

Windows computers provide an additional location for setting the path environment variable. To change the path on a Windows computer, open the system Control Panel, click Advanced System Settings, and click the Environment Variables button. You can use the Environment Variables dialog box to modify the path for the computer.

## *Putting it together*

[Listing 5-3](#) is a short batch file that has been documented with `rem` (remark) statements throughout the file. It shows a completed file that uses many of the techniques discussed in this section. This batch file was designed to gather a list of 32-bit programs installed on a computer (by getting a directory listing of the 32-bit Program Files directory) and to gather the TCP/IP configuration from a computer and place it in a text file on the `c:` drive; but it could place the information on a drive on a server so that it could be collected by an administrator. The text file that the batch file creates is named for the computer information from which the information was gathered. This data is collected only once. The networking troubleshooting commands used in this file can be found in Book 8, [Chapter 3](#).

## **LISTING 5-3 Batch File Documented with `rem` Statements**

---

```
rem Check for existing file, and if it exists, exit the batch file,
rem and make the directory if it does not exist.
if not exist C:\Settings\nul mkdir C:\Settings
if exist C:\Settings\%computername%.txt goto end
rem Check to see if the computer is running Windows 64-bit (amd64)
rem or Windows 32-bit (x86).
if not !%PROCESSOR_ARCHITECTURE%==!AMD64 goto 64bit
:32bit
rem Create a new file containing the output of the two settings
rem which is the current TCP/IP Configuration.
ipconfig /all >> C:\Settings\%computername%.txt
rem Add to this file the current routing table using netstat.exe
netstat.exe -r >>> C:\Settings\%computername%.txt
rem Add to this file the output of the correct Program Files directory
dir /ad "%ProgramFiles%" >>> C:\Settings\%computername%.txt
rem Skip the Windows 64bit section and goto the end of the file.
goto end
:64bit
rem Use Windows 64-bit OS path to the 32-bit Program Files directory
rem networking commands.
winipcfg /all /batch C:\Settings\%computername%.txt
netstat.exe -r >>> C:\Settings\%computername%.txt
dir /ad "%ProgramFiles(x86)%" >>> C:\Settings\%computername%.txt
:end
```

If this file is saved to `C:\Windows\GetSettings.bat`, it can be executed by specifying the name of the file `GetSettings` in a command window or by typing it after choosing `Start ⇒ Run`. By specifying the name, the entire path on your computer will be searched for the file with `.com`, `.exe`, `.cmd`, or `.bat` as the file extension.

## ***Working with VBScript***

Without going to third-party solutions, Windows was limited to batch files for automation prior to the release of Visual Basic Scripting (VBScript) around 1996, shortly after which it was included automatically with the



Windows OS. As the name suggests, it is based loosely on Visual Basic. While not as powerful or fast as a Visual Basic application, VBScript offers the following benefits: It is easy to write programs in, it does not require a compiler to operate, and it does not require a custom application to be installed to be able to write a program (you only need `notepad.exe`), although code aware software such Notepad++ or a VBScript aware IDE (Integrated Development Environment) can make writing your script much easier.

The main competition to VBScript when it was released was from JavaScript, which offered many of the same benefits as VBScript, but JavaScript required the installation of Java support on your computer.

## *Calling a script*

While I said you do not need to compile your scripts in VBScript, you do need to use a command interpreter to execute them. Microsoft provides two interpreters with the Windows OS:

- » `wscript.exe`: This is a Windows-based interpreter. When you double-click your script to execute it, it will run using Windows Script. Some commands in your script will behave differently if you are using `wscript` over `cscript`.
- » `cscript.exe`: This is a command-line interpreter and is run from a command window (`cmd.exe`). The default output location for `cscript.exe` is called `stdout`, and it is the command window. This allows you to use commands like `wscript.echo` to send data to the command window when your script is running.

If you want to change the default script interpreter for Windows, typing **`cscript //H:CScript`** in a command window, while typing **`cscript //H:WScript`** will put you back to the OS default.

To execute, run, or call the script, you can double-click in Windows Explorer to launch it with the default interpreter, or you can type in the name of the interpreter followed by the path to and name of the script in the Run command or in a command window, like **`cscript C:\MyScripts\Test-script.vbs`**. If you use this command in the Run

command, the script will run in a command window, and the window will close when the script completes. So if you want to see the output, run the script from an open command window.

## *Script structure*

Most programming languages follow a common structure that breaks down into four basic sections. These are Declarations, Main, Functions, and Subroutines. Within each of these sections are the lines of programming that will make your script or program function.

### *Declarations*

Most programs will have a number of variables or constants with which they will work. The Declarations section is where you will put these items. Think of it like algebra: “Let  $X = 5$ ” and “Solve for  $Y$ .” In most languages, variables and constants may contain numbers, strings (text), or Boolean values. While some programming languages require that you state the type of value you are going to place in a variable, VBScript declares all variables automatically as variant. This means that they could hold a variety of types of values. Here are a few variables that are defined in a script; three variables are set, two are used for strings (which are enclosed in quotes), and one is for an integer. After defining the variables, `strFilePath` and `iPrinterCount` have values set:

```
Dim strFilePath, strDataRow
Dim iDoPrtrSize
strFilePath = "N:\temp\"
iPrinterCount = 0
```

Constants differ from variables in that they cannot change, like  $\pi$  or the speed of light. In programming, when you declare a constant for use, you will define the value to use at the same time. Here is a series of constants that will be used when working with files in VBScript:

```
Const OPEN_FILE_FOR_READING = 1
Const OPEN_FILE_FOR_APPENDING = 8
Const OPEN_FILE_FOR_WRITING = 2
Const CREATE_FILE_IF_NEEDED = 1
Const OVER_WRITE_FILE = 1
```

The other item that gets declared in this section are objects. Objects are a little different than variables in that they contain properties (which hold values) and methods (actions that they can perform). Two of the common objects you will use in your scripts are `Scripting.FileSystemObject` and `WScript.Shell`. The File System object is used to manipulate files on your hard drive. You would use this to copy or move files, as well as to open, write to, and close text or binary files. The Shell object allows you to access system environment variables and to run commands (other programs). Here you define a variable and associate an object with it through the `set` command. Later you will create a file object and save data to the file.

```
Dim oFileSystem
Set oFileSystem = CreateObject("Scripting.FileSystemObject")
```



**WARNING** VBScript will actually allow you to use variables without first declaring them, which can cause problems if you are fat-fingered. The following script is an example of this problem:

```
Dim strMyName, strNamePlus
strNyName = "Ed Tetz"
strNamePlus = strMyName & " is awesome."
```

Now, if you go to use the variable `strNamePlus`, you will expect it to contain “Ed Tetz is awesome.” when it actually contains “is awesome.” This script will not generate an error letting you know that a problem exists, but it will not function the way you expect. The solution is `option explicit`, which forces you to declare all variables that you will be using. If you attempt to run a previous script with `option explicit`, when you attempt to run the script, you will see an error, telling you that an undeclared variable existed.

### *Main procedure*

The main part of the program or script is all the Main procedure. When the script executes, this is where the main flow of logic comes from. In VBScript, the main function starts automatically after the variables are

declared and continues until a `WScript.Quit(0)` is encountered. In some languages, the Main procedure is identified by name.

Good programming practice typically means that the Main procedure will be short and identifies the main flow of the program. Most of the work done by the script will be in the form of subprocedures and functions.

### *Subprocedures or subroutines*

A subprocedure or subroutine is a section of a program that performs a set of commands and returns to the subprocedure or function that called it. It is like giving a task to someone to complete, and when the task is done, the person comes back to you to tell you it is done. You can define locally used variables at the start of the subprocedure in the same way that you declared variables for use at the start of the Main procedure. You can pass parameters to a subprocedure, or the subprocedure could have no parameters. When passing parameters, you can use values or variables when calling subprocedures. [Listing 5-4](#) shows what a simple subprocedure would look like; this sample includes a section of the Main procedure and makes use of the message box function to display results.

#### **LISTING 5-4 A Simple Subprocedure**

---

```
Dim iNumOne, iNumTwo
iNumOne = 5
iNumTwo = 6
AddNumbers iNumOne, iNumTwo
WScript.Quit(0)
Sub AddNumbers (iFirstNum, iSecondNum)
    Dim iTotal
    iTotal = iFirstNum + iSecondNum
    MsgBox iTotal
End Sub
```

Here are a few things to make note of in this example:

- » **Local variables:** `iFirstNum`, `iSecondNum`, and `iTotal` are local variables that only exist inside of the `AddNumbers` subprocedure.
- » **Passing variables:** `iNumOne` and `iNumTwo` are values that are passed to variables `iFirstNum` and `iSecondNum` in the `AddNumbers`

subprocedure.

- » **Passing values:** Rather than passing values stored in variables, you can also call the `AddNumbers` subprocedure with values, like `AddNumbers 3, 6`.
- » **Ending the subprocedure:** Procedures and many other structures have both a starting and an end; in many cases, the end uses the control word `end`.

## *Functions*

A function is similar to a subprocedure with one major difference: A function returns a value to the calling procedure. Any type of calculation can be performed within the function, and those results can be passed back. So take a look at the last script being changed to a function in [Listing 5-5](#). Notice that the message box is now in the Main procedure, using the value returned from the function.

### **LISTING 5-5 A Simple Function**

---

```
Dim iNumOne, iNumTwo, iTotal
iNumOne = 5
iNumTwo = 6
iTotal = AddNumbers(iNumOne, iNumTwo)
MsgBox iTotal
WScript.Quit(0)

Function AddNumbers (iFirstNum, iSecondNum)
    AddNumbers = iFirstNum + iSecondNum
End Function
```

Here are a few things to make note of in this example:

- » **Brackets:** Brackets surround the parameters in a function. This defines for VBScript that you are using a function and that a value will be returned.
- » **Function variable:** The function name is treated like a variable within the function, and this is used to set the value that will be returned by the function.

Because [Listing 5-5](#) had you set `iTotal` and use that in a message, you can optimize your code a bit by eliminating that `iTotal`, which you see in [Listing 5-6](#).

### **LISTING 5-6 Streamlined Function**

---

```
Dim iNumOne, iNumTwo
iNumOne = 5
iNumTwo = 6
MsgBox AddNumbers(iNumOne, iNumTwo)
WScript.Quit(0)

Function AddNumbers (iFirstNum, iSecondNum)
    AddNumbers = iFirstNum + iSecondNum
End Function
```

## ***Decisions and Boolean logic***

When you have a program that is going to perform a task for you, you will probably have the program perform some type of decision making along the way. To perform these decisions, you will use Boolean logic to make these decisions. Two main decision structures that are used are `If` and `Case`.

The `If` statement opens with an `If` and a condition (which is evaluated to see whether it is true) and closes with an `End If`. Two other optional elements are in the statement: `ElseIf` and `Else`. `Else` is the action to take if the `If` condition is not met, whereas `ElseIf` combines an `Else` with another `If` statement. If you have used an `ElseIf`, you are still able to use an `Else`. [Listing 5-7](#) shows an example of a complete `If` statement.

### **LISTING 5-7 If Statement**

---

```
Dim a, b, c
a = 5
b = 5 + 2
If a > b Then
    c = a
ElseIf b > a Then
    c = b
Else
```

```
        c = a + b
    End If
```

[Listing 5-8](#) shows the `Select Case` statement, which is similar to `If` statements in that they make decisions. But they are used to evaluate the contents or results of a single statement rather than different criteria at each `ElseIf` statement.

### **LISTING 5-8 Select Case Statement**

---

```
Dim Name
Name = "Bobby"
Select Case Name
Case "Jane"
    MsgBox "Jane is awesome."
Case "Judy"
    MsgBox "Judy is great."
Case "Bobby"
    MsgBox "Bobby is the best."
End Select
```

## ***Loops***

If something is worth doing, it is worth doing again, and again, and again. In most cases, within your program or script, you will want to repeat certain steps several times. Perhaps you want to perform an action on every text file in a folder, or perform a step 100 times, or perform an action until a certain condition is met. If this is the case, you would like to loop.

### ***For Next***

The `For Next` loop works with a counter to loop between two values, using an increment or step value, with the default value being 1. The loop repeats every command from the `For` statement to the `Next` statement. Notice that in [Listing 5-9](#), the value of `i` is joined (or concatenated) with the string by using the ampersand (&), which is used to join strings or string variables together.

### **LISTING 5-9 For Next Loop**

---

```

Dim i
For i = 2 to 10 step 2
    MsgBox "The current value of i is: " & i
Next

```

## ***For Each Next***

The `For Each Next` loop requires a collection of some sort to function. These collections may be created on the fly by inspecting an object, such as the files in a folder of the `FileSystemObject` or the properties of a file. The other item that may be used for a collection is an array. To keep things easy, in [Listing 5-10](#) you create an array that will be used for the looping.

### **LISTING 5-10 For Each Next Loop**

---

```

Dim Egg, Eggs(2)
Eggs(0) = "Robin"
Eggs(1) = "Eagle"
Eggs(2) = "Hawk"
For Each Egg in Eggs
    Wscript.echo "The current egg is: " & Egg
Next

```

Unlike the `For Next` loop, which increments a value, this loop will cycle through the collection of objects until the collection is complete.

## ***While***

The `While` loop continues the loop while the test condition remains to be true. The items in the loop condition need to be modified in the looping process so that there is a chance that the condition will eventually become false. Unlike other statements that have an `End`, the `While` loop ends with a `While End`, or rather `Wend`. [Listing 5-11](#) provides a sample of this loop.

### **LISTING 5-11 While Loop**

---

```

Dim i
i = 0
While i < 10
    Wscript.Echo "The current number is: " & i
    i = i + 1
Wend

```



Wend

While the `While` loop is still used by some people in VBScript, it is on its way out of favor in preference for the `Do Loop` command, which achieves the same results.

## ***Do Loop***

The `Do Loop` command supports either `While` or `Until` conditions, which may be tested either at the start of the loop or at the end of the loop. The four options for looping that you could use are shown in [Listing 5-12](#).

### **LISTING 5-12 Do Loop**

---

```
Dim i
i = 0
Do While i < 10
    Wscript.Echo "The current number is: " & i
    i = i + 1
Loop

i = 0
Do Until i >= 10
    Wscript.Echo "The current number is: " & i
    i = i + 1
Loop

i = 0
Do
    Wscript.Echo "The current number is: " & i
    i = i + 1
Loop While i < 10

i = 0
Do
    Wscript.Echo "The current number is: " & i
    i = i + 1
Loop Until i >= 10
```

## ***Screen output***

If you want to view what is going on in your script, you can send output to the screen. You can use two basic commands: One is the message box (`MsgBox`) command, and the other is the `Wscript.echo` command.

### *Wscript.echo*

The `echo` command simply tells your script to send a copy of the data you provided to the standard output of the script interpreter. For `wscript.exe`, this would be a message box, while `cscript.exe` will send the output to the command window. For scripts that generate a lot of output, you will want to run them through `cscript.exe` to avoid a huge series of message boxes.

### *MsgBox*

The `MsgBox` option will work through either `cscript.exe` or `wscript.exe`. This command will open a message box on the screen with a provided title, message, and buttons. This command can be called as subprocedure or as function, with the function returning the value of the button that is clicked in the message box. Brackets enclose the parameters of the function, while if it is called without brackets, it will operate as a subprocedure and not return that value. Here is the syntax of the `MsgBox` command:

```
MsgBox(prompt[,buttons][,title][,helpfile,context])
```

Note the square brackets, identifying options, where `prompt` is the only required parameter for the command. If no title is given, the default Windows Script Host is used.

For buttons, the default is an OK button, but you can choose to display multiple buttons in your message box; this is only useful if you are using it as a function. You can use either the constant name or the number for the button parameter:

- » **0:** `vbOKOnly`: OK button only
- » **1:** `vbOKCancel`: OK and Cancel buttons
- » **2:** `vbAbortRetryIgnore`: Abort, Retry, and Ignore buttons
- » **3:** `vbYesNoCancel`: Yes, No, and Cancel buttons

- » 4: `vbYesNo`: Yes and No buttons
- » 5: `vbRetryCancel`: Retry and Cancel buttons
- » 16: `vbCritical`: Critical Message icon
- » 32: `vbQuestion`: Warning Query icon
- » 48: `vbExclamation`: Warning Message icon
- » 64: `vbInformation`: Information Message icon

If you want to display a message box with `vbOKCancel` buttons and have the message box show a `vbQuestion` icon, add the two numbers together and use `1+32`, `vbOKCancel+vbQuestion`, or `33`, as the button parameter.

Putting in more than the OK button only makes sense if you are going to do something with the information, so you will use the `MsgBox` as a function and get information back regarding the button pressed. This function will return the following values if the matching button is pressed:

- » 1: `vbOK`: OK was clicked
- » 2: `vbCancel`: Cancel was clicked
- » 3: `vbAbort`: Abort was clicked
- » 4: `vbRetry`: Retry was clicked
- » 5: `vbIgnore`: Ignore was clicked
- » 6: `vbYes`: Yes was clicked
- » 7: `vbNo`: No was clicked

[Listing 5-13](#) has an example of this function in action. Note the use of `vbCRLF` to break the prompt into two lines and the underscore to break the line into two pieces for readability (the extra spaces on the second line are ignored).

### **LISTING 5-13 Message Boxes**

---

```
Dim Answer
Answer = MsgBox("Is blue your favorite color." & vbCRLF & "Answer
               honestly.", _
```

```

vbYesNo +vbQuestion , "Favorite Color")
if Answer = vbYes then
    WScript.echo "Blue is your favorite color."
Else
    WScript.echo "Your favorite color is not blue."
End If

```

By implementing message boxes as functions, you can control the flow of operations in your script.

## *Opening and saving files*

You have already been introduced to the `FileSystemObject`, at least in principle. Now you take a look at a couple of things you can do with this object, specifically opening a file to read data and opening a file to write data into a file. In [Listing 5-14](#), you read the contents of a file, add a line number to the beginning of each line, and write these lines of data back out to another file.

### **LISTING 5-14 Reading Files**

---

```

Dim oFSO, oReadFile, oWriteFile, TextLine, i
Const ForReading = 1
Const ForWriting = 2
Const ForAppending = 8
i = 1
Set oFSO = CreateObject("Scripting.FileSystemObject")
Set oReadFile = oFSO.OpenTextFile("C:\Temp\InputFile.txt", ForReading)
Set oWriteFile = oFSO.CreateTextFile("C:\Temp\OutputFile.txt", True)
Do Until oReadFile.AtEndOfStream
    TextLine = oReadFile.ReadLine
    oWriteFile.Write i & " " & TextLine & vbCRLF
    i = i + 1
Loop
oReadFile.Close
oWriteFile.Close

```

## *Working with parameters*

You can do only so much inside a script without needing to make changes to it. To reduce the number of times that you need to make changes to a

script, you can call the script with arguments (also called parameters). [Listing 5-15](#) is an example of working with arguments within a script.

### **LISTING 5-15 Working with Arguments**

---

```
args = WScript.Arguments.Count
If args < 1 then
    WScript.Echo "Usage: args.vbs argument [argument] [argument] [argument]"
    WScript.Quit
end If
WScript.Echo "You entered " & args & " arguments and they are as follows."
For i = 0 to args - 1
    WScript.Echo " Argument number " & i & " is " & WScript.Arguments.Item(i)
Next
```

The arguments that the script receives can then be put into variables to be used through the rest of the script.

### ***Executing external commands***

From within your script, you may want to run another command at the OS level. In [Listing 5-16](#), you perform a directory listing in a new window and leave that window open. The directory that is listed is provided by a variable in the script, but it could also be provided as an argument.

### **LISTING 5-16 Executing External Commands**

---

```
Dim oShell, directory
directory = "C:\Temp"
Set oShell = WScript.CreateObject("WScript.Shell")
oShell.run "cmd /K CD " & directory & " & Dir"
Set oShell = Nothing
```

The last line of the script is a bit of cleanup, where you destroy the object that was created earlier.

### ***Forcing a stop***

When running your scripts, at times the script will get into a loop or generate a series of message boxes that seem to never end. If you want to

stop a running script, open Task Manager and navigate to the Processes tab. Now locate the `wscript.exe` process, right-click, and choose End Process. This will terminate the script where it is.

## *Getting More Power with Windows PowerShell*

PowerShell is a new scripting language developed by Microsoft, and I use “new” relatively, as PowerShell was released in 2006. Microsoft released PowerShell as an update to VBScript and to offer a new command-line management interface for new OS and server functions. In addition to the language itself, Microsoft also created a series of commands, or cmdlets, to perform a series of preset functions.

PowerShell is a feature on current Windows OSes.

### *Calling a script*

If you run `powershell.exe` by itself, you will enter interactive mode, where you can issue cmdlets or commands, such as `get-Command`, to get a listing of the installed cmdlets. You can also run these commands from the command line using the format of `powershell.exe get-Command`. I introduce you to some Windows OS cmdlets later; these represent much of the power of PowerShell. Different components installed on your computer can install their own PowerShell console and cmdlets; this would include Microsoft Exchange and VMware vSphere.

As with VBScript, you can create a text file containing a series of commands, loops, and conditional statements, and then execute this script file from the command line. These script files have an extension of `.ps1` and can be called using this command:

```
powershell.exe C:\Temp\MyScript.ps1
```

Before you are able to run a script, you need to ensure that the Execution Policy allows you to execute scripts. Run the command `Get-ExecutionPolicy`. If it is set to `Restricted`, you will need to change it, which you can do with the following command:

When you run this command, you will need to confirm the security change. If you are on a managed computer, then you may not be able to change the execution policy. When not running scripts, Restricted is a safer setting for your computer.

## *Cmdlets*

Much of the power of PowerShell lies in the cmdlets. One cmdlet you should know is `Get-Help`. Cmdlets are named telling you what their actions will do. They start with an action or verb (like `Add`, `Set`, or `Get`) and end with a noun (like `Computer`, `EventLog`, or `Service`).

All commands have modifiers or parameters that can be used. When running your commands to retrieve data, you can filter the output by including these parameters. [Listing 5-17](#) shows the output of the `Get-Service` command, with a restriction showing only some of the services. Notice the `*` wildcard used in the command.

### **LISTING 5-17 Working with Cmdlets**

---

```
PS C:\temp> Get-Service -Name Remote*

Status Name DisplayName
-----
Stopped RemoteAccess Routing and Remote Access
Stopped RemoteRegistry Remote Registry
```

Output from this command can be passed to another command by way of the pipe symbol (`|`). In [Listing 5-18](#), you will pipe to the `Format` command to format the output. In PowerShell, pipe is also called *pipeline*.

### **LISTING 5-18 Working with Pipe**

---

```
PS C:\temp> Get-Service -Name Remote* | Format-Wide

RemoteAccess RemoteRegistry
```

## *Script structure*

Some people will say that PowerShell is sloppy, while others will say it is free-form and efficient. Unlike VBScript, which is very structured in its format, PowerShell offers a lot of flexibility.

## *Declarations*

Unlike VBScript, in PowerShell you do not declare your variables; you simply start using them. You can, however, start using them right away, but if you want to be more formal, you can use the `Set-Variable` command. When using variables, you will use the `$` operator to identify them:

```
Set-Variable -Name strMyName -Value "Ed Tetz"  
$strTrait = "is an author."
```

A number of characters are not allowed in variable names: `! @ # % & , .` and spaces. Additionally, certain reserved keywords used in PowerShell are not allowed to be used as variable names: `break`, `continue`, `do`, `else`, `elseif`, `filter`, `foreach`, `function`, `if`, `in`, `return`, `switch`, `until`, `where`, and `while`.

Although it is a good idea, it is not required to start a variable name with the type of data that you are storing in the variable. This includes strings (`strName`), integers (`intAge` or `iAge`), and Boolean (`bCorrect`), to name a few. Naming your variables this way avoids keyword conflicts and lets you keep track of the data that is found in the variable.

While PowerShell will attempt to decide on the fly what types of variables you are working with, you do have the option of hard-coding the variable types by declaring your variables like this:

```
[str]$strMyName="Ed Tetz"
```

Other variable types would be

- » **array:** Array of values
- » **byte:** 8-bit character
- » **bool:** Boolean value
- » **char:** Unicode 16-bit character
- » **decimal:** 128-bit decimal value



- » **double:** 64-bit decimal number
- » **hashtable:** Hashtable object
- » **int:** 32-bit signed integer
- » **long:** 64-bit signed integer
- » **single:** 32-bit decimal number
- » **str:** Fixed-length string of Unicode characters
- » **xml:** XML object

### *Main procedure and functions*

One big difference between VBScript and PowerShell is how you code the main procedure and functions. Function blocks can be created anywhere in your code, but it is good form to place all your functions at the start of your script. In most cases, you need to define the function before you use the function.

If you are in the middle of your script and you need to exit immediately, a command is available to you. In VBScript, you could use `WScript.Quit(0)`, but in PowerShell, you have the `break` command.

The `break` command has a partner in the `continue` command. If you want to exit the current function, loop, or main procedure, you can use `break`. Every structure with separated code, be it a function or a loop, will be enclosed in braces `{ }`. If you place a `break` within that block, the block will immediately be exited. If the `break` command is used outside all blocks, the main procedure will be exited. The `continue` command is a little different from the `break` command. Like the `break` command, the `continue` command could be used in a loop; but rather than exiting the loop entirely, the `continue` command will skip over all remaining commands in the loop and return to the beginning of the loop for the next iteration.

So a short script would look like the code sample in [Listing 5-19](#).

---

### **LISTING 5-19 PowerShell Scripts**

```
$x = 5
```

```
$y = 6
$Ans = $x + $y
Write-Host "The answer is $Ans"
```

If you wanted to use a function, the code sample would look more like [Listing 5-20](#).

## **LISTING 5-20 PowerShell Function**

```
Function AddNums ($Num1, $Num2)
{
    $Ans = $Num1 + $Num2
    return $Ans
}
$x = 5
$y = 6
$x = AddNums 5 6
"The Answer is $x"
```

## ***Decisions and Boolean logic***

When making decisions in Windows PowerShell, you will need to be familiar with the comparison operators, which you can find in [Table 5-2](#).

**TABLE 5-2 Comparison Operators**

<b><i>Operator</i></b>	<b><i>Description</i></b>
-eq	Equal to
-lt	Less than
-gt	Greater than
-le	Less than or equal to
-ge	Greater than or equal to
-ne	Not equal to
-ieq	Text comparison, case insensitive equal to
-ceq	Text comparison, case sensitive equal to

Boolean operators can also be used to modify the returned values and change the result of a Boolean comparison. These operators are listed in

[Table 5-3.](#)

**TABLE 5-3 Boolean Operators**

<i>Operator</i>	<i>Description</i>
-not	Not
!	Not
-and	And
-or	Or

[Listing 5-21](#) has a sample of the `If Elseif Else` operator. It allows you to control actions that occur in your script. Notice that test arguments are enclosed in parentheses, and braces `{ }` are used for the commands related to each portion of the `If`.

### **LISTING 5-21 If Statement**

---

```
$a = 5
$b = 5 + 2
If ($a -gt $b)
{
    $c = $a
}
Elseif ($b -gt $a)
{
    $c = $b
}
Else
{
    $c = $a + $b
}
Write-Host $c
```

The equivalent statement to VBScript's `Select Case` is the `Switch` statement. This statement starts with the variable that you are comparing and then the list actions to perform at each matching value. If no values are matched, no action is taken, but you are allowed to use a default action as a catchall if you would like, as in [Listing 5-22](#).

## **LISTING 5-22 Switch Statement**

---

```
$Name = "Bobby"
Switch ($Name)
{
    "Jane" {Write-Host "$Name is awesome."}
    "Judy" {Write-Host "$Name is great."}
    "Bobby" {Write-Host "$Name is the best."}
    default {"$Name, I am not familiar with that person"}
}
```

## ***Loops***

To allow you to perform steps a repeated number of times, several options are available to you. Here are the most common types of loops you will use in PowerShell.

### ***Do While***

The main looping structure in PowerShell is `Do`. `Do` identifies the start of the looping structure, which continues through a pair of braces. At the end of the braces, you find the `While` condition. The loop will always process once with the evaluation to repeat the process being made at the end.

When the contention is true, looping continues. [Listing 5-23](#) shows a `Do While` loop.

## **LISTING 5-23 Do While Loop**

---

```
$i = 1
Do
{
    Write-Host $i
    $i++
} While ($i -le 5)
```

Notice the `$i++` found in this code; this is shorthand that was used with C++. This is short for `$i = $i + 1`. If you need to perform the reverse calculation, `$i = $i - 1`, you can use the `$i--` shorthand.

### ***Do Until***

Similar to the previous loop, the loop in [Listing 5-24](#) repeats until the conditions are met.

## **LISTING 5-24 Do Until Loop**

---

```
$i = 1
Do
{
    Write-Host $i
    $i++
} Until ($i -gt 5)
```

The only difference between `Do While` and `Do Until` is that your criteria for evaluation is reversed between the `While` and `Until` loops. While these two loops have used a countermechanism, any logic test could have been used to exit the loop, such as the length of a string or a variable containing a certain value.

### ***For***

The `for` loop repeats through a process for a fixed number of iterations. In this case, the criteria put all the loop logic into a single block of logic associated with the `For` command. The block `($i=1;$i -le 5;$i++)` has three commands that perform the same counter functions that were used in the previous two loops. First you set `$i` to 1, you evaluate to see whether `$i` is less than or equal to 5, and then you add 1 to the value of `$i`. As long as `$i` is less than or equal to 5, you perform the actions within the braces, as illustrated in [Listing 5-25](#).

## **LISTING 5-25 For Loop**

---

```
For ($i=1;$i -le 5;$i++)
{Write-Host $i}
```

### ***ForEach***

As the name suggests, the `ForEach` loop performs an action for each item that exists in an array or a collection. In [Listing 5-26](#), you use the `Get-Process` cmdlet to get a collection of process objects, which you can then perform an action upon.

## **LISTING 5-26 For Each Loop**

---

```
ForEach ($item in Get-Process)
{Write-Host $item.Name}
```

## Screen output

Getting a PowerShell script to report information is quite easy. You have four basic methods of getting a script to write information to a location:

- » Quote a string
- » Write-Output command
- » Redirect symbol
- » Write-Host

The easiest way to have a script generate output is to put a quoted string on a line of the script, which will cause that to be outputted on the screen. To report a variable or a string with a variable embedded, simply put them alone on a line in your script. [Listing 5-27](#) is an example of these commands. Notice that you simply put the variable inside the string, whereas in VBScript, you need to concatenate the text and variables together.

### **LISTING 5-27** Outputting to the Screen

---

```
"My Name"  
$strMyName = "Ed Tetz"  
$strMyName  
"My name is $strMyName"
```

This output will show up on the screen or wherever `stdout` (standard output) is set to display output. The other way to get data sent to `stdout` is with the `Write-Output` command:

```
Write-Output $strMyName
```

Rather than having the data sent to the screen, you can have `stdout` redirect data to a file by using the redirect symbol (`>`). This can be done for specific commands or for an entire script. Here are a couple of examples:

```
C:\Temp\MyScript.ps1 > C:\Temp\Output1.txt  
"My name is $strMyName" > C:\Temp\Output2.txt
```

When redirecting output to an alternate location, you can use `Write-Host`, which will force output to the screen:

```
Write-Host $strMyName
```

## *Opening and saving files*

Rather than using redirection, you may also use the `Out-File` command to specifically write data to a file. Here you use the `Out-File` command to save the output from the `Get-Processes` command by passing the data through a pipe:

```
Get-Processes | Out-File C:\Temp\Processes.txt
```

If you want to append to a file, if it already exists, rather than overwriting the file, you use the `Append` option:

```
Get-Processes | Out-File -Append C:\Temp\Processes.txt
```

The `NoClobber` option is a little different; it says that if the file already exists, do not overwrite the file. In this case, the original file will remain intact and the new file will not be saved:

```
Get-Processes | Out-File -NoClobber C:\Temp\Processes.txt
```

Like the `Out-File` command, the `Export-Csv` command sends output to a file, but in this case, it will be a comma-separated values (`.csv`) file, which can then be opened in Microsoft Excel or Notepad:

```
Get-Processes | Export-Csv C:\Temp\Processes.csv
```

Getting data from a file is easy with PowerShell. The `Get-Content` command allows you to read the contents of a file and treat the content as a collection. [Listing 5-28](#) has you put the content of the file into a collection named `$Names`:

### **LISTING 5-28 Getting Content from Files**

---

```
$Names = Get-Content "C:\Temp\Names of People.txt"
ForEach($Name In $Names)
{
    Switch ($Name)
    {
        "Jane" {Write-Host "$Name is awesome."}
```

```
"Judy" {Write-Host "$Name is great."}
"Bobby" {Write-Host "$Name is the best."}
default {"$Name, I am not familiar with that person"}
}
}
```

Because you were able to export data to a CSV file, it is good to know that you are able to get data in from a CSV file. The `Import-Csv` command reads data from the file and allows you to use it immediately:

```
Import-Csv C:\Temp\Processes.csv
```

## *Working with parameters*

When you create a script, you may want to reuse it by using arguments (also called parameters). To use arguments when calling scripts, you only need to know how to work with the `$Args` array. [Listing 5-29](#) is an example using a script named `Test.ps1`.

### **LISTING 5-29 Managing Arguments**

---

```
"The number of arguments are:"
$args.count
"Here is the list of arguments:"
ForEach ($arg in $args)
{
    $arg
}
"Here is another way to list arguments:"
For ($i=0;$i -lt $args.count;$i++)
{
    $args[$i]
}
```

To call this script, you would use a command similar to the following:

```
Powershell.exe C:\Temp\Test.ps1 One Two Three
```

## *Executing external commands*

From time to time, you will want to use a script to execute commands at the OS level. While you have many ways to do this, here are a couple of ways that you can do this with PowerShell, which includes `Start-Process` and `&`. Both of these examples open a text file with Notepad:

```
Start-Process "notepad.exe" "C:\Temp\MyFile.txt"
&"notepad.exe" "C:\Temp\MyFile.txt"
```



## *Power of pipeline*

One of the overlooked functions in PowerShell is the pipeline feature, which allows you to pass output from one command into another. While you have seen the pipeline earlier in this chapter, it is worth seeing another demonstration that applies condition statements and loops.

If you were using a language other than PowerShell, or if you did not use pipeline, then you might have a script like [Listing 5-30](#). This script does the following:

- » Defines an object collection, which includes all services
- » Loops through each object (each is a service)
- » Checks whether the current object matches search criteria, which are services in a stopped state and have a name of VSS or W32Time
- » Starts services that match the criteria

### **LISTING 5-30 Start Service Script**

---

```
$objServices = Get-Service
ForEach ($objService in $objServices)
{
    If ($objService.Status -ieq "Stopped" -and ($objService.Name -ieq "VSS" -or
        $objService.Name -ieq "W32Time"))
    {
        Start-Service $objService.Name
    }
}
```

Thanks to pipeline, this entire loop can be condensed to one line. The first part of the command gets the collection of services, the second part has the filter condition to all services, and the third part starts any services that make it through the filter. Pipelining of commands gives PowerShell the ability to do a lot with few lines of code, like this:

```
Get-Service | ?{ $_.status -ieq "Stopped" -and ($_.name -ieq "VSS" -or $_.name -
    ieq "W32Time")} | Start-Service
```



ON THE  
WEB

Labs 5-1 and 5-2 guide you through using PowerShell commands and creating a PowerShell script. The labs can be found on the companion website at [www.dummies.com/go/aplusaio](http://www.dummies.com/go/aplusaio).

## *Shell (.sh) Script*

In the Linux environment you can create scripts to automate the administration of the Linux system. The type of script in Linux is known as Shell Script. Shell script files have a `.sh` extension and can be created with any text editor in Linux such as the `vi` editor or `nano`. Within the shell script you can place Linux commands to perform Linux tasks for you.

In a text editor you start your shell script with the following line. It is an important line of code because it specifies the interpreter for the script:

```
#!/bin/bash
```

You then can write the rest of your script using Linux commands and scripting constructs. Like other scripting languages you have common elements to a script such as variables, decision structures, and loops. Let's have a look at each of these.

### *Variables*

As you learn earlier, a variable is a temporary storage space for information that you will use later in the script. To create a variable in shell script, you can use the following command:

```
strName = "Glen E. Clarke"  
echo $strName
```

The first line stores a string into the variable called `strName`, while the second line of code prints the variable contents onto the screen. With shell script if you want to prompt the user for information and store what the user types as a response into a variable you can use the `read` command as in:

```
#!/bin/sh
```

```
echo What city are you from?
read CITY
echo "You are from $CITY, hope the weather is nice there!"
```

In this example, the `read` command is used to read input and place that input into the variable called `CITY`. Anytime you want to use the variable within your script you place a `$` in front of the variable name as in `$CITY`.

## *Decision structures*

We also have decision structures like `if` statements in shell script. The basic syntax for an `if` statement in shell script is:

```
if [ $AMOUNT -gt 100 ]; then
    # put commands here
fi
```

Notice that with the `if` statement, you have the test you are performing within square brackets `[ ]` then a `;` to keep the `then` on the same line as `if`. Inside the `if` statement you specify the commands to execute if the condition is found true. To end the `if` statement, use `fi`. You can also run commands if the condition is found false if you add `else`:

```
if [ $AMOUNT -gt 100 ]; then
    # put true commands here
else
    # put false commands here
fi
```

If you wanted to perform multiple test with an `elseif` statement in shell script, you would use the following code:

```
if [ $AMOUNT -gt 100 ]; then
    # put commands here
elif [ $AMOUNT -lt 10 ]; then
    # put commands here
else
    # put commands here
fi
```

Note that in order to do an `elseif` you use the keyword `elif`.

## *Loops*

Like other scripting languages, you can also have loops within shell script. The reasoning for loops is the same as what was discussed in the other languages discussed earlier in the chapter, but the syntax is a bit different.

### *For loop*

A `for` loop is used to loop through a set of values. In this example, I am looping through the numbers 1, 2, 3, and 4 where `$i` will hold one of those values each time through the loop, and then printing the value:

```
for i in 1 2 3 4
do
    echo "Printing number: $i"
done
```

### *While loop*

The `while` loop is used to execute a block of code while the condition is found true. In this example I am prompting for a city while I continue to prompt the user for a city until the city is equal to Halifax:

```
while [ "$CITY" != "Halifax" ]
do
    echo "Please type your favorite city"
    read CITY
    echo "Your favorite city is: $CITY"
done
```

Note the `do` at the beginning of the code that is to execute, and the `done` line to identify the end of the loop.

### *Executing the script*

Once you have typed your commands into the script file, save the file with a `.sh` extension. In order to execute the script, you will need to ensure that you have the execute permission on the file. To give execute permission on the file type the following:

**\$ `chmod 755 script1.sh`**

Once you have the permission to execute the script, you can execute it by referencing the script file by its name, including the path to the file:

\$ ./script1.sh

## *Python Script*

Another common scripting environment is Python. In order to execute scripts in Python you need to ensure that you have installed the Python interpreter on your system. Note that most Linux distributions have Python installed, but you will have to install it on most Windows systems. You can install Python for Windows from

<https://www.python.org/downloads/windows>.

To create your first Python script, launch your favorite text editor and type the following:

```
print('First Python Program')
name = input('What is your name?')
print('Welcome, ',name, '. We hope you like Python scripting!')
```

The first line of code is used to print a message to the screen, in this case a title for the screen. Then you prompt the user for his or her name with the input function and store whatever they type into a variable called name. Then you print out a welcome message using that name.

After creating the code for your script file, you can then save it with a .py extension.

## *Variables*

When working with variables in Python you do not declare the variables with a data type like you do with some other languages. Python determines the data type based on the data that is assigned to a variable. For example, when you assign a value that has single quotes around it, Python treats that as a string value and not an integer, float, or Boolean.

The following code would assign create a variable of a string data type:

```
name = 'Glen Clarke'
```

The following code would create a variable of an integer (numeric) data type:

```
age = 10
```

The following code would create a variable of a Boolean (true or false) data type:

```
married=false
```

## *Decision structures*

Once data is assigned to variables, you typically want to perform a set of commands based on if a test is found true or false. Like the other scripting languages, we have `if` statements. To write a basic `if` statement you start with the keyword `if` and then specify your condition followed by a colon (:). You then write all the code that is to execute if that condition is found true:

```
numdays = int(input("How many days in a week? "))
if numdays == 7:
    print("You got it right!")
```

To write an `if...else` statement, you follow the same structure but add an `else` block with the `else:` statement and then the code that is to execute if the condition is found false. Here is an `if...else`:

```
numdays = int(input("How many days in a week? "))
if numdays == 7:
    print("You got it right!")
else:
    print("I am sorry, you are incorrect.")
```

If you want to perform multiple tests, you can use the `if...elif` (for `elseif`) logic of:

```
numdays = int(input("How many days in a week? "))
if numdays == 7:
    print("You got it right!")
elif numdays == 3:
    print("3 is incorrect.")
else:
    print("I am sorry, you are incorrect.")
```

## *Loops*

Like the other languages, we have loops in Python such as a `for` loop and a `while` loop.

The `for` loop is used to loop through a known set of values. In this example, I am storing a number of names into a variable and then looping through the names to print them out:

```
names = ['Glen','Bob','Sue']
for iter in names:
    print('Name: ',iter)
```

With this `for` loop, the variable `iter` represents each individual name as you loop through all the names. To print the name, you print the variable `iter`.

The `while` loop is how you can loop based on a condition. In this example, I continuously prompt the user for a score until he or she types 0 as a score:

```
score = 1
while score != 0 :
    score = int(input("Enter score? [0 to exit]"))
    print("Student score is: ",score)
```

## *Executing the script*

In order to execute a Python script, you first need to navigate to the command prompt and call the `python.exe` program and then pass in as a parameter the path to your script. For example:

```
C:\>python.exe c:\myscripts\firstscript.py
```

## *JavaScript*

The final scripting language to discuss is JavaScript. JavaScript is a common scripting language found with web development and can be executed from a hosting application such as a web browser.

The good news is that from a syntax point of view JavaScript is similar PowerShell so there is not a lot of new code to learn here. A few things you should know about JavaScript before looking at some code examples are that JavaScript is case sensitive and each statement ends with a semicolon (;).

## *Variables*

Variables in JavaScript can hold different types of data such as numbers or strings. You can create a variable by first declaring the variable:

```
var age;
```

You can then assign a value to the variable with:

```
age = 10;
```

or

```
name = "Glen Clarke"
```

In the first example, a number is being stored in the age variable (no quotes), while in the second example text information (string data) is stored in the name variable.

If you wanted to, you could declare and assign the variable all in one step with the following code:

```
var age = 10;
```

## *Decision structures*

If statements in JavaScript are similar to other languages with a few minor adjustments. Here is the structure of a basic `if` statement in JavaScript. The first thing to notice is that the condition is in parentheses ( ), and the block of code to execute if the condition is found true is in the curly bracket section { }:

```
var workyears = 10;  
if (workyears < 10) {  
    raise = 1.15;  
}
```

You can add an `else` section to execute if the condition is found false:

```
var workyears = 10;  
if (workyears < 10) {  
    raise = 1.15;  
} else {  
    raise = 1.25;  
}
```



If you want to perform multiple tests, you can use an `else if` statement as in the following example:

```
var workyears = 10;
if (workyears < 10) {
  raise = 1.15;
} else if (workyears < 20) {
  raise = 1.25;
} else {
  raise = 1.50;
}
```

Notice with the `else if` statement that you must supply a new condition within the circular brackets to test upon.

## *Loops*

Two main loops in JavaScript are the `for` loop and the `while` loop. The `for` loop is used to loop through code a set number of times, while a `while` loop is used to loop through code based on a condition.

You start the `for` loop with the keyword `for` and then there are three parameters separated by colons within the circular brackets. The first part is an initializer that creates a variable to be used by the loop and assigns it an initial value. Then you have a condition to stay in the loop — in my code example, I stay in the loop `while i < 5`. The final parameter of the `for` loop is the incrementer, which specifies that `i` is to be incremented by 1 (`i++`):

```
for (i = 0; i < 5; i++) {
  // statements here
}
```

You also have a `while` loop in JavaScript that works the same way as the `while` loop in other languages. The difference is that the condition is in circular brackets:

```
while (score != 0) {
  // statements here
}
```

# Commenting Your Code

It is a common practice to add comments to your code in order to give a brief description of what the code does. This is important because if you or someone else reviews the script months or years later, you may need to give a reminder as to what the purpose of the code is.

When putting a comment in your code you must precede the comment with a comment symbol so that the scripting environment knows not to try to execute that line. For example, in Powershell you use the # symbol to comment code:

```
#Retrieve the BIOS information from the local system  
Get-WMIObject win32_bios
```

Each scripting language uses a different symbol or method to comment out code. [Table 5-4](#) shows the different comment symbols used to add comments to code.

**TABLE 5-4** Comment Syntax Symbols

Language	Symbol	Function
Batch File	rem	The rem command is used add a comment to code in .bat files.
VBScript	'	A single quote mark is how you create a comment in VBScript.
PowerShell	#	A hash symbol is how you create a comment in PowerShell.
Shell Script	#	A hash symbol is how you create a comment in Shell script.
Python	#	A hash symbol is how you create a comment in Shell script.
JavaScript	//	The // symbols are used to comment a single line in JavaScript.

## Getting an A+

This chapter introduced you to a new exam objective added to the 2019 version of the A+ exams — scripting. It introduced to you some of the major scripting environments in Windows, Linux, and MacOS. Be sure to review these key points when preparing for the A+ exams:

- » Older Windows operating systems use batch files and VBScript as a way to automate tasks.
- » PowerShell is the new scripting environment for Windows and should be a big focus of yours for the exam. Shell scripts and Python scripts are common on Linux systems.
- » A `for` loop is used to loop through a set of values; a `Do Loop` or a `while` loop is used to loop through code based on a condition. A `for each` loop is used to loop through an array or collection.
- » You can use conditional structures such as an `if` statement to branch into other code based on a condition.
- » You can store information temporarily into variables for later processing. In some scripting environments such as Windows PowerShell, variables have data types, such as integer or string, assigned to them.
- » You can add comments to your code, which are lines of code that are not executed. Comments are a good way of adding documentation to your code.

## *Prep Test*

**1. You are creating a PowerShell script and would like to print a message to the screen; what command would you use?**

- (A) `Read-host`
- (B) `Print`
- (C) `Write-Host`
- (D) `Printf`

**2. You are creating a PowerShell script that needs to read the contents of a file; what command would you use?**

- (A) `Read-Content`
- (B) `Get-Content`
- (C) `Read-File`

(D) `Get-File`

**3. Which of the following commands would you use to execute a PowerShell script?**

(A) `./firstscript.ps1`

(B) `firstscript.ps1`

(C) `./firstscript.py`

(D) `firstscript.py`

**4. Which of the following represents the proper syntax for an `if` statement in Shell script?**

(A) `if [$age > 40]`

(B) `if ($age > 40)`

(C) `if ($age -gt 40)`

(D) `if [$age -gt 40]`

**5. You are receiving a permission error when trying to execute a Shell script; what should you do?**

(A) Assign the execute permission

(B) Assign the read permission

(C) Assign the modify permission

(D) Assign the write permission

**6. What command would you use to execute a Python script?**

(A) `c:\scripts\firstscript.ps1`

(B) `python.exe c:\scripts\firstscript.ps1`

(C) `python.exe c:\scripts\firstscript.py`

(D) `python.exe firstscript.py`

**7. You need to comment code within your JavaScript; which of the following represents the syntax you would use?**

- (A) `rem`
- (B) `//`
- (C) `#`
- (D) `'`

## Answers

1. **C.** To print information on the screen in PowerShell you would use the `write-host` command. See “[Screen output.](#)”
2. **B.** The `get-content` command is used to read the contents of a file. Review “[Opening and saving files.](#)”
3. **A.** To execute a PowerShell script, you simply type the name of the `.ps1` file including its path. Check out “[Calling a script.](#)”
4. **D.** The `if` statement in shell script uses square brackets and comparison operators such as `-eq`, `-gt`, `-lt`, and `-ne`. Peruse “*Shell (.sh) Script.*”
5. **A.** In order to execute a shell script, you must assign the execute permission on the file. Take a look at “*Shell (.sh) Script.*”
6. **C.** To execute a Python script, you reference the `python.exe` program and then pass in as a parameter the full path to the script file, which has a `.py` file extension. Peek at “[Python Script.](#)”
7. **B.** Comments in JavaScript start with `//`. Look over “[JavaScript.](#)”

# Book 7

# Recovering Systems

## Contents at a Glance

### Chapter 1: Managing Error Codes and Startup Messages

[Windows Boot Files and Failure-to-Boot Errors](#)

[Solving Linux Boot Issues](#)

[Device-Related Errors](#)

[Other Errors](#)

[Error Diagnostic Tools](#)

[Getting an A+](#)

[Prep Test](#)

[Answers](#)

### Chapter 2: Managing Common Problems

[Solving Windows-Specific Service Problems](#)

[Solving Boot Errors and Errors Requiring Restarting](#)

[Resolving Device Driver and Service Errors](#)

[Application Install, Start, and Load Failures](#)

[Solving Linux File-Related Problems](#)

[Solving Other Problems](#)

[Getting an A+](#)

[Prep Test](#)

[Answers](#)

### Chapter 3: Preparing for Disasters with Disaster Recovery

[Using F8 Options during Boot-Up](#)

[Emergency Repair](#)

[Understanding Backup and Restore](#)

[Recovery and Rescue Methods](#)

[Scheduling Preventive Maintenance](#)

[Getting an A+](#)

[Prep Test](#)

[Answers](#)

# Chapter 1

## Managing Error Codes and Startup Messages

---

### IN THIS CHAPTER

- » Recognizing and resolving common error codes and startup messages
  - » Resolving issues with missing boot files or OS components
  - » Identifying steps to correct operational problems
  - » Using diagnostic utilities and tools to resolve operational problems
- 

This chapter examines problems common to the Windows environment. Many of these problems occur during the boot process, but a few can occur at any time. I examine boot or startup errors first and then other errors that occur within the OS. The end of the chapter reviews some tools used to help diagnose the cause of the errors.

As an A+ Certified Professional, you will often need to diagnose problems based on error codes and messages from the OS. This chapter introduces you to many common boot or startup error messages that you might see when using Windows. You also are introduced to the key files required to allow you to boot a computer running Windows.

## *Windows Boot Files and Failure-to-Boot Errors*

All operating systems are vulnerable to issues that can keep them from booting, and the current crop of Windows OSes, from Windows 7 on, is



no different. The following sections look at some of these problems and possible resolutions.

Officially, the CompTIA A+ exam objectives list post-Windows Vista OS versions — namely, Windows 7, Windows 8.1, and Windows 10.

However, even though the 1000-series objectives don't reference Windows XP boot files, for completeness' sake, I cover them here. After all, as much as it pains me to say it, some of my PC hardware work is on Windows XP systems that Microsoft stopped supporting long ago!



**TIP**

To help you understand the key files that are used in the boot process, you may want to review Book 5, [Chapter 6](#).

The Windows boot process can suffer from boot sector corruption, boot loader problems, and drive identification problems within `boot.ini` or the Boot Configuration Database (BCD). For most problems, the Emergency Repair Process or the Windows Recovery Environment (RE) are reasonable troubleshooting and repair steps. (I discuss the Emergency Repair Process and the Windows RE in [Chapter 3](#) of this minibook.)

## ***No operating system found or incorrect boot device***

The No operating system found error in Windows is tied to severe corruption of the boot sector on your hard drive. To restore your drive to working condition, perform the Emergency Repair /Startup Repair process to restore the boot sector on your hard drive. This feature is called “Startup Repair” in Windows 7, Windows 8.1, and Windows 10.

The Startup Repair process is covered in Book 7, [Chapter 3](#). Minor corruption of the boot files would report missing files, such as `winload.exe` or `ntoskrnl.exe`, and the next section tells you how to deal with missing files. The No operating system found error could be caused by an improperly set BIOS/UEFI boot order.

If you have multiple hard drives, flash drives, or USB devices connected to your computer, they may have been placed higher in the boot order than your normal boot drive. If that is the case, you may see messages related

to missing boot files. If this is the case, your solution to the issue is to enter the BIOS/UEFI configuration on your computer and select the correct device to be used as the boot device. The solution may be simpler with removable devices, because the device can simply be removed.



TECHNICAL  
STUFF

I have had one computer that would attempt to use my iPhone as a boot device when it was connected; as you can guess, this did not work very well.

## *Missing boot files*

Windows requires several core files to boot, and an optional file. The required files are

- » `ntldr` (Windows XP)
- » `ntdetect.com` (Windows XP)
- » `boot.ini` (Windows XP)
- » `bootmgr` (Windows Vista, Windows 7, Windows 8.1, Windows 10)
- » Boot Configuration Database (BCD) (Windows Vista, Windows 7, Windows 8.1, Windows 10)
- » `winload.exe` (Windows Vista, Windows 7, Windows 8.1, Windows 10)
- » `ntoskrnl.exe` (Windows Vista, Windows 7, Windows 8.1, Windows 10)

The optional file is

- » `ntbootdd.sys`, which is the SCSI adapter driver that Windows XP boots from if the SCSI adapter doesn't have its own BIOS

In the following sections, you get a look at what you can do if any of these files are missing or appear to be missing on your computer.

## *ntldr*

As I state earlier, NTLDR is the boot loader for Windows XP and the previous versions in the Windows New Technology (NT) OS line. NTLDR worked in conjunction with NTDETECT.COM, which performed hardware detection, and boot.ini, which pointed NTLDR to your Windows installation.

From Windows Vista forward, Microsoft replaced NTLDR with `bootmgr.exe` and `winload.exe`. Instead of recording the `\Windows` directory location in `boot.ini`, post-XP systems read startup information directly from the boot configuration database (BCD); this data can be read and modified by using the `bootcfg` utility.

If `ntldr` is missing on a Windows XP system, you will receive the following error message when your computer tries to boot:

```
NTLDR is missing
Press any key to restart
```

This message often means that the computer is attempting to boot from a device that has no boot loader present. If this file is actually missing, it can be replaced with a working copy from any pre-Windows Vista computer, although try to replace the missing file with a copy from the same or a newer version of Windows to maintain full compatibility. To replace this file, you can boot the system from the Windows DVD and perform an Emergency Repair/Startup Repair process.

## *boot.ini*

If the `boot.ini` file is missing and you installed Windows XP in its default location, the system will boot but will not display a boot menu. The default location for the OS in Windows XP and newer versions of Windows is `c:\windows`. If you have not installed Windows in its default location, you will receive a message stating that `ntoskrnl.exe` or `hal.dll` is corrupted or missing and that you should replace the file. The message will look similar to this, from Windows XP, stating that a DLL file is missing:

```
Windows could not start because the following file is missing or corrupt:
<Windows root>\system32\hal.dll
```

Please re-install a copy of the above file.

This message is misleading because the problem is really with the `boot.ini` file. The reason for the message is that the boot loader (`ntldr`) has gone to the default location, and `ntoskrnl.exe` or `hal.dll` files were not there. If the `boot.ini` file is replaced and the boot path is correct for your installation, the boot process will continue as normal.



**REMEMBER** `boot.ini` is a text file and can be edited with any text editor, such as `notepad.exe`. To replace the `boot.ini` file, you might need to create a boot disk like you did to replace the missing `ntldr` file.

### ***ntdetect.com***

If `ntdetect.com` is missing, you receive the following error message:

NTDETECT failed

This file is generic, like the `ntldr` file, and can be replaced in the same way that you replace the `ntldr` file. See the earlier section, “[ntldr](#).”

### ***bootmgr***

Windows Vista introduced a brand-new way to start the Windows operating system. Instead of `ntldr` orchestrating the boot process, Windows Vista through Windows 10 rely upon a file named `bootmgr` located on the system partition. The `bootmgr` file then reads the Boot Configuration Data (BCD) store, again on the system drive, to determine how to complete the Windows OS load.

If `bootmgr` is missing, you receive the following error message when your computer tries to boot:

BOOTMGR is missing  
Press Ctrl+Alt+Del to restart

To resolve this type of error, look at using the Startup Repair process or the repair Command Prompt with tools like `bootrec.exe /fixboot`. For more information about the Startup Repair process as well as repairing errors, see [Chapter 3](#) of this minibook.

## ***Boot Configuration Database (BCD)***

The BCD data store is located on the EFI System Reserved Partition for UEFI systems, and in the `C:\boot\BCD` directory for BIOS systems.

If the BCD is missing, you receive the following error message when your computer tries to boot:

```
Windows Boot Manager
Windows failed to start. A recent hardware or software change might be the
cause. To fix the problem:
1. Insert your Windows installation disc and restart your computer.
2. Choose your language settings, and then click "Next."
3. Click "Repair your computer."
If you do not have this disc, contact your system administrator or computer
manufacturer for assistance.
File: \Boot\BCD
Status: 0xc000000f
Info: An error occurred while attempting to read the boot configuration
data.
Enter=Continue ESC=Exit
```

To resolve this type of error, look at using the Startup Repair process or the repair Command Prompt, which includes tools like `bootrec.exe` /`RebuildBCD`, or `bcdedit.exe`. `bcdedit.exe` will allow you to manually rebuild the BCD.

In Windows 10, you can access Startup Repair by starting the system from your Windows DVD (or USB stick if you created startup media), and selecting Repair your computer from the Welcome screen.

## ***winload.exe***

From Windows Vista onward, `winload.exe` (or `winload.efi` on UEFI systems) loads the Windows OS executive (`ntoskrnl.exe`) and the core device drivers into memory. As such, `winload.exe` is a crucial system file.

If `winload` is missing, you will receive the following error message when your computer tries to boot:

```
Windows Boot Manager
Windows failed to start. A recent hardware or software change might be the
```

```
cause. To fix the problem:
1. Insert your Windows installation disc and restart your computer.
2. Choose your language settings, and then click "Next."
3. Click "Repair your computer."
If you do not have this disc, contact your system administrator or computer
manufacturer for assistance.
File: \Windows\system32\winload.exe
Status: 0xc000000f
Info: The selected entry could not be loaded because the application is
missing or corrupt.
Enter=Continue ESC=Exit
```

To resolve this type of error, look at using the Vista Startup Repair process or the repair Command Prompt, which includes tools like `bootrec.exe /RebuildBCD`, or `bcdedit.exe`. `bcdedit.exe` will allow you to manually rebuild the BCD.

### ***ntoskrnl.exe or hal.dll***

You should be able to find the `ntoskrnl.exe` file in the `windows\system32` directory. If it's missing, you receive a message like this from Windows:

```
Windows could not start because the following file is missing or corrupt:
<Windows root>\system32\hal.dll
Please re-install a copy of the above file.
```

These messages may look familiar; they are the same messages that you receive if your `boot.ini` file is misconfigured. After checking the `boot.ini` file, if the `ntoskrnl.exe` or `hal.dll` files are actually missing, you have to do one of the following:

» **Perform an Emergency Repair Process.** Use Startup Repair in Windows Vista or later to replace any missing or corrupted files on your system.

For more information on the Emergency Repair Process, see Book 7, [Chapter 3](#).

» **Attempt to replace the file by using the Recovery Console.**

» **Re-install the operating system.**



**REMEMBER** Ninety-nine out of 100 times, the missing `ntoskrnl.exe` or `hal.dll` error message means an error with the `boot.ini` file or the BCD, and the `ntoskrnl.exe` or `hal.dll` file is fine. While `hal.dll` represents a missing `dll` file, many other `dll` files are integral to the OS operating correctly. If many of these are missing, the recovery option will be through the Emergency Repair/Startup Repair process, which is covered in [Chapter 3](#) of this minibook.

## *Solving Linux Boot Issues*

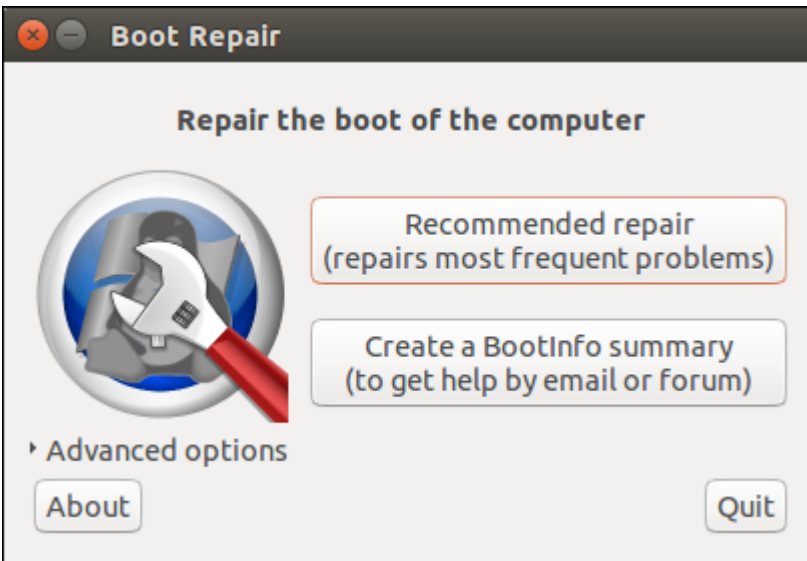
One big change CompTIA made to the 900-series A+ exam objectives that remains in the 1000-series exams is fairly heavy coverage of Linux. This makes sense to me because you'll encounter Linux quite a bit in business, especially in enterprise servers.

Let's examine a few common startup-related issues you may see in Linux, and discuss how to solve them quickly.

### *Missing GRUB/LILO*

LILO and GRUB are the two main boot loader packages used in Linux. Nowadays GRUB is used almost exclusively. In my experience, the most common cause for a Linux system "losing" its boot loader is when you attempt to dual-boot between Linux and Windows. In this case, Windows often removes the GRUB loader in order to replace it with its own.

The good news is that you can easily re-enable GRUB. The specific instructions depend upon your Linux distribution, but the general procedure is to (1) start the computer from the Linux installation media; and (2) run a graphical or Terminal-based bootloader repair tool. For example, in Ubuntu Linux you can easily install the GUI tool Boot-Repair (shown in [Figure 1-1](#)) to re-install GRUB easily.



**FIGURE 1-1:** Ubuntu Linux is known for being simple to use. Even re-installing the GRUB boot loader is easy, thanks to the Boot Repair tool.

## *Graphical interface fails to load*

If a Linux system boots to the Terminal, you should verify that the system actually has a graphical environment like GNOME installed in the first place. Many Linux systems administrators, for example, refuse to load GUI shells on servers in order to keep the system running as “leanly and meanly” as possible.

For most Linux distributions, you can manually start the graphical shell from a Terminal by running the `startx` command.

## *Missing graphical interface*

What if your Linux system doesn’t have the graphical shell installed? You may need to configure an Ubuntu Linux system, but due to time pressures you need to at least temporarily load the graphical desktop to enact the repair.

Once again, Ubuntu Linux makes the process super easy. From the Ubuntu Terminal, run the following command:

```
sudo apt-get install -re-install ubuntu-desktop
```

Here, I break down each part of the previous Linux Terminal command:



- » `sudo`: This stands for “superuser do,” and instructs Ubuntu to run the command as the superuser as opposed to a standard user.
- » `apt-get install`: The Advanced Packaging Tool (apt) is one of the most popular Linux package managers. You use apt tools to find, install, maintain, and remove software, all from the command line.
- » `ubuntu-desktop`: This is a single apt package that bundles the Ubuntu graphical desktop environment.

## *Device-Related Errors*

It is unfortunate that the devices and their drivers that allow us to accomplish so much of our day-to-day work with computers are also one of the biggest factors in not being able to do work on our computers. Ideally, when all the devices are configured on your computer, you should be able to work with no problems from your drivers.

Most people's computers don't remain in a static mode but are in constant flux. Even though devices are working fine, many people feel the need to try to improve performance by changing settings, upgrading drivers, or installing Service Packs.

Although upgrading drivers and installing items such as Service Packs are common practice, they should be done carefully. A Service Pack, for instance, can change how all drivers on your computer function. In the rare case when something does go wrong, you may find that the fix is difficult, but in most cases, it will be related to a file version or configuration setting. This section takes a look at how to address these problems.

### *A device referenced in system files is not found*

From time to time, you will find that one of your startup files still references a device that you thought had been removed from your system. The Windows Registry holds all configuration references for installed devices. If this happens, you might have to edit the Registry manually in order to fix the problem. If an error message tells you that a referenced

device does not exist, take note of the device being referenced because you will have to search for it in your startup files.

If the device is listed in the Registry, as it should be nowadays, it should be listed in Device Manager. I like to describe Device Manager as a “candy-coated front end” to the Windows Registry. Generally, it’s safer to make Registry changes through Control Panel than by using the Registry Editor directly.

Choose Start ⇒ Control Panel ⇒ System, click the Hardware tab of the resulting dialog box, and then click the Device Manager button. For Windows Vista and Windows 7, choose Start ⇒ Control Panel ⇒ System and Security ⇒ Device Manager. Locate the device in Device Manager and delete it. If the device is still physically present in the computer, it will be re-added to Device Manager when your computer is rebooted. If you keep removing the device and it keeps coming back, that is because it is still physically present. Physically remove the device first, and then remove it from Device Manager.

In Windows, if you do not see the device that you want to remove in Device Manager, choose Show Hidden Devices from the View menu. If you can’t find the device in the Windows GUI, you can attempt to search the Registry to locate the device and correct the issue. To find out about editing the Registry, see Book 6, [Chapter 4](#).

## ***Registry corruption***

The two main ways that the system Registry can become corrupted are updates to the Registry via one of the Registry editing tools or an import of a registry settings file, and by the files that make up the Registry becoming damaged or deleted.

Of the many ways to import data into the Registry, most of them involve storing settings in a file and importing that file into the Registry. If the settings in the file are incorrect, you might be able to just continue computing without any problems, or you could end up with a system that no longer boots normally. If your system will not boot normally, your only option is to boot the system by using an alternative method, such as the

Recovery Console, and replace the base Registry files with an untainted version.

You also need to use an alternative method to boot the system if the Registry files on the drive itself have become corrupted, and then you have to replace the Registry files. The user portion of the Registry — `ntuser.dat` — is found in your user profile directory. Your user profile directory is in `C:\Users\<username>` for Windows Vista and beyond.

The system portion of the registry is found in

`%systemroot%\system32\config`, in the files `SAM`, `SECURITY`, `system`, and `software`. For information about editing the Registry, see Book 6, [Chapter 4](#).

## *Safe Mode*

In order to let you repair the OS from within the OS, Microsoft provides Safe Mode. *Safe Mode* is available with most versions of Windows and is a special boot of Windows that loads a minimal set of drivers and services. The only drivers that are loaded are the ones that are required to get the OS running. Instead of loading the normal video driver, Safe Mode loads a basic VGA graphics driver. If you have issues with drivers or driver configuration, booting into Safe Mode can allow you to bypass these driver-related problems so that they can be fixed.

Safe Mode should be your “go to” boot mode when you’re repairing a system that’s been infected by malware. In Safe Mode you don’t have Internet access because Windows hasn’t loaded any network drivers; this prevents the infected system from “phoning home” and counteracting your malware removal techniques.

In Windows 7 and later, you can boot into different Safe Mode variants. For instance, you can load Safe Mode with or without networking support. Alternatively, you can skip the Windows Desktop and boot to a Safe Mode Command Prompt.

Enter Safe Mode by pressing the F8 key when the OS is booting (Windows 7), or by holding the Shift key when you issue the shutdown command from the Start menu (Windows 8.1 and Windows 10). If your computer boots into Safe Mode, the words `Safe Mode` appear in each

corner of your desktop. If Windows fails to boot properly, it will suggest — and attempt — to boot into Safe Mode on the next boot. If your computer boots into Safe Mode automatically, the last boot process was likely interrupted (usually by the user). For more information about Safe Mode and other boot methods, consult Book 7, [Chapter 3](#).

## *Other Errors*

Like with all things in life, some things cannot easily be categorized, so this section discusses errors that do not fit in the other categories in this chapter.

### *Paging file errors*

The Windows *paging file* is a hard drive file that is used as additional RAM memory. Typically, with Windows, the file is called the paging file or page file, but some people may use “swap file” instead (that’s the typical Linux term).

The location of the paging file is recorded in the Registry. If the drive that contains the paging file becomes too full, you might encounter errors informing you of this fact. If this happens, create some additional space for the paging file by deleting some unnecessary files, reducing the size of the paging file, or moving the paging file to a new location. The default location for the paging file is in the same drive as your Windows directory. Windows allows you to move the paging file to an alternate drive. If you have done so and that drive has been removed from your system, you encounter errors telling you that the paging file could not be created. If this happens, configure Windows to use another drive for the paging file as shown in Book 6, [Chapter 3](#).

### *Failure to start GUI*

Sometimes, Windows cannot complete the boot process, but it will not generate an error, either. Instead, it seems to hang at one spot in the boot process without going any further. You can deal with this problem in a number of ways.

First, see whether the OS has loaded the networking components, which you can do using the `ping` utility discussed in Book 8, [Chapter 3](#). If the networking services are running, you might be able to connect to the computer using Computer Management or Event Viewer, as described in Book 6, [Chapter 4](#), which will allow you to view information about the OS and read the event logs. The event log might show errors that let you know what the problem is.

If you cannot connect to the computer, your only options are to continue to wait or to cycle the power on the computer. If the computer has locked up hard enough, the soft power button might not work, and you might have to unplug the computer. For a laptop, you have to remove the battery.



**WARNING** This action, like any power interruption, risks causing corruption to the file system, and should be used as a last resort.

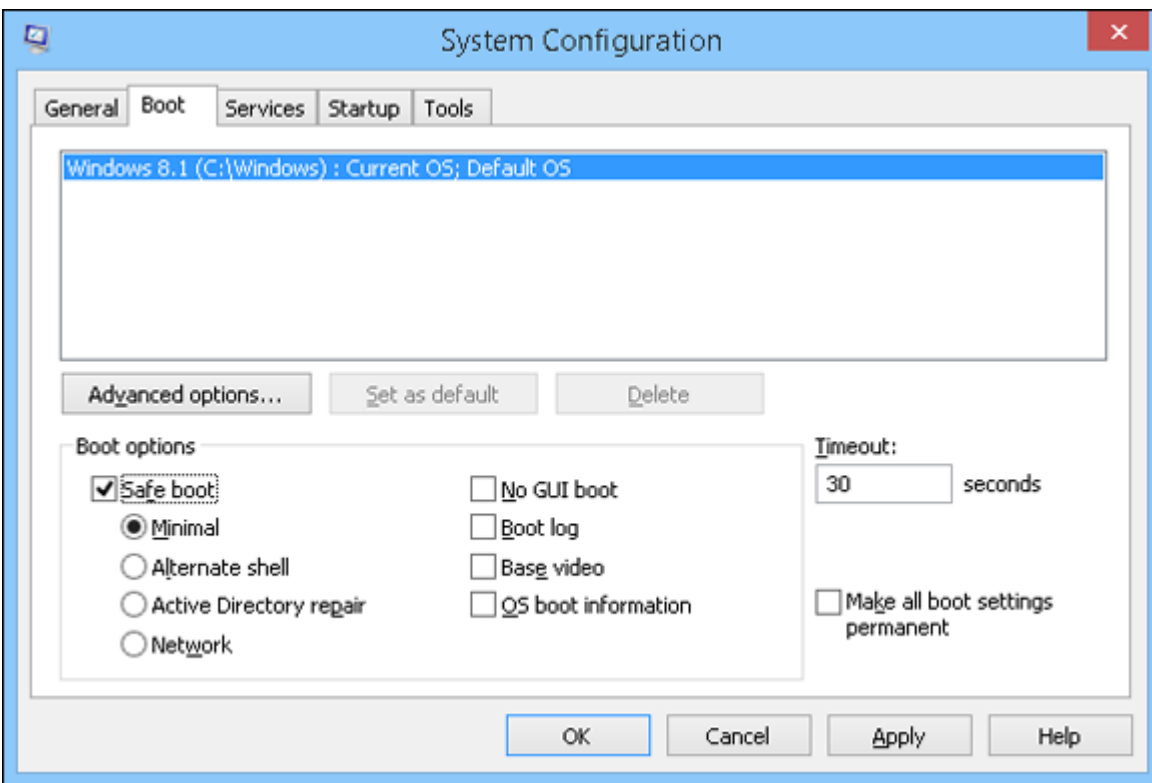
On reboot, the system might boot properly, or you might want to use one of the F8 boot options discussed in Book 7, [Chapter 3](#), such as Safe Mode. Safe Mode allows you to view the Event Logs via Event Viewer, and that might give you insight into the problem. The F8/Shift boot options also allow you to create a bootlog, which if your next boot is unsuccessful, will let you know approximately where the failure has occurred. If you are unable to find the solution, disconnect all peripherals (such as USB devices) and attempt to reboot the computer. If the problem is with a peripheral or its driver, you might see a successful boot. In some cases, I have seen errors with peripherals occur after the system has successfully booted for years, and the problem can usually be traced to an OS update, a drive update, or file system corruption of the driver.

If you think you know what is causing the problem, perhaps a driver or service that will not start, you could also use Recovery Console to try to fix those problems. For more information about Recovery Console and its use, consult Book 7, [Chapter 3](#).



**TIP**

On newer, faster systems, getting the timing right for the F8 startup keystroke can be incredibly difficult. If this is the case, consider opening the System Configuration Utility, shown in [Figure 1-2](#), and specifying the Safe Boot option. In Windows 8.1 and Windows 10, you can navigate to the Start menu, hold down the Shift key, click the Power button, and select Restart. Fast and easy!



**FIGURE 1-2:** Type **msconfig** from a Windows command prompt to open the System Configuration utility. From here you can force-boot into Safe Mode.

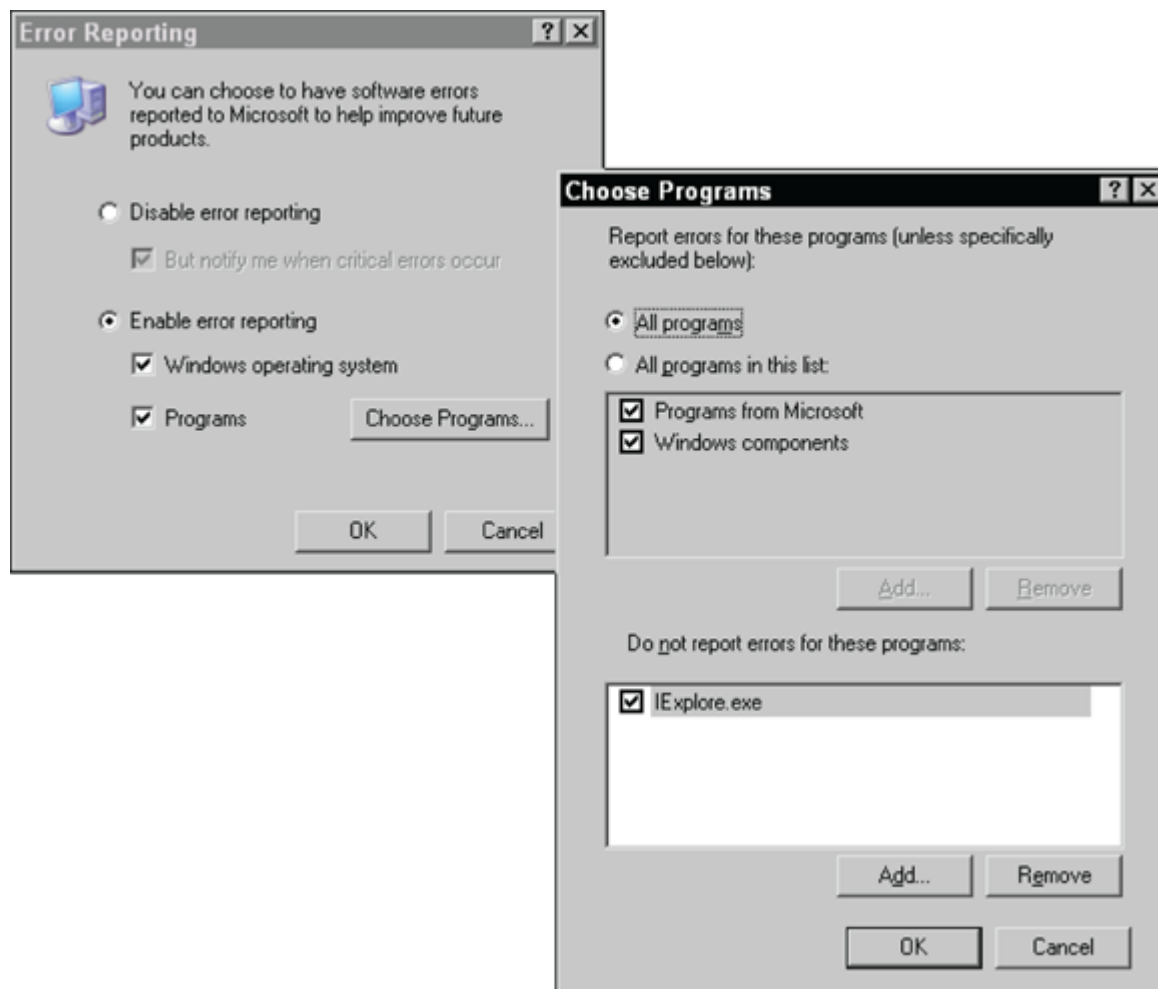
## *Error Diagnostic Tools*

The following sections examine the different tools you can use when diagnosing errors.

### *Windows Error Reporting*

With Windows XP, Microsoft introduced the Error Reporting Tool, which is a tool for error reporting that replaced most of the functionality originally covered by Dr. Watson in “prehistoric” Windows versions. The Error Reporting tool allows you various levels of reporting. The idea is that when an application or the operating system itself crashes, Windows sends anonymous technical data to Microsoft, where programmers can identify bugs and ultimately update the Windows code base to the benefit of all customers.

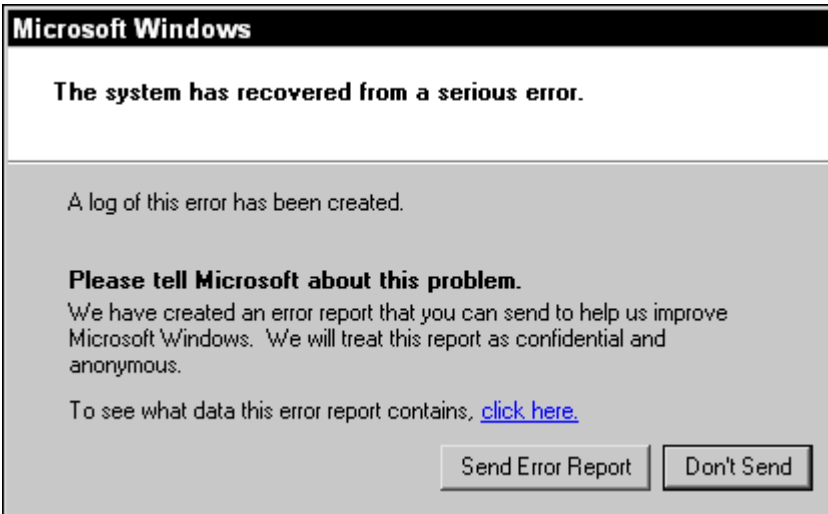
By default, it is configured to report errors in both applications and the OS directly to Microsoft, which allows its programmers the potential to use the information when creating new patches for the operating system. This “call home” functionality can be disabled in Windows by going to the Error Reporting button on the Advanced tab of the System Control Panel applet. Clicking the Error Reporting button opens the Error Reporting dialog shown in [Figure 1-3](#). From this dialog, you can disable the “call home” functionality but still have Windows report the errors to you; specify that Error Reporting works for both OS components and programs; or use the Choose Programs button to specify which programs you want to have Error Reporting work with, or exclude.



**FIGURE 1-3:** Windows Error Reporting helps Microsoft fix problems with the OS.

When an application crashes, you will see a message similar to the one in [Figure 1-3](#). If Windows has a Stop error, though (described in Book 7, [Chapter 2](#)), you see the message after you reboot and log in. Click the link at the bottom of the dialog box to find additional information related to the error. When you see this dialog, you can send a summary of the error data and system state to Microsoft, as shown in [Figure 1-4](#). If you disabled Error Reporting but kept the notify option enabled, you get a smaller dialog box without the option for notifying Microsoft, but only an OK button to acknowledge the error.



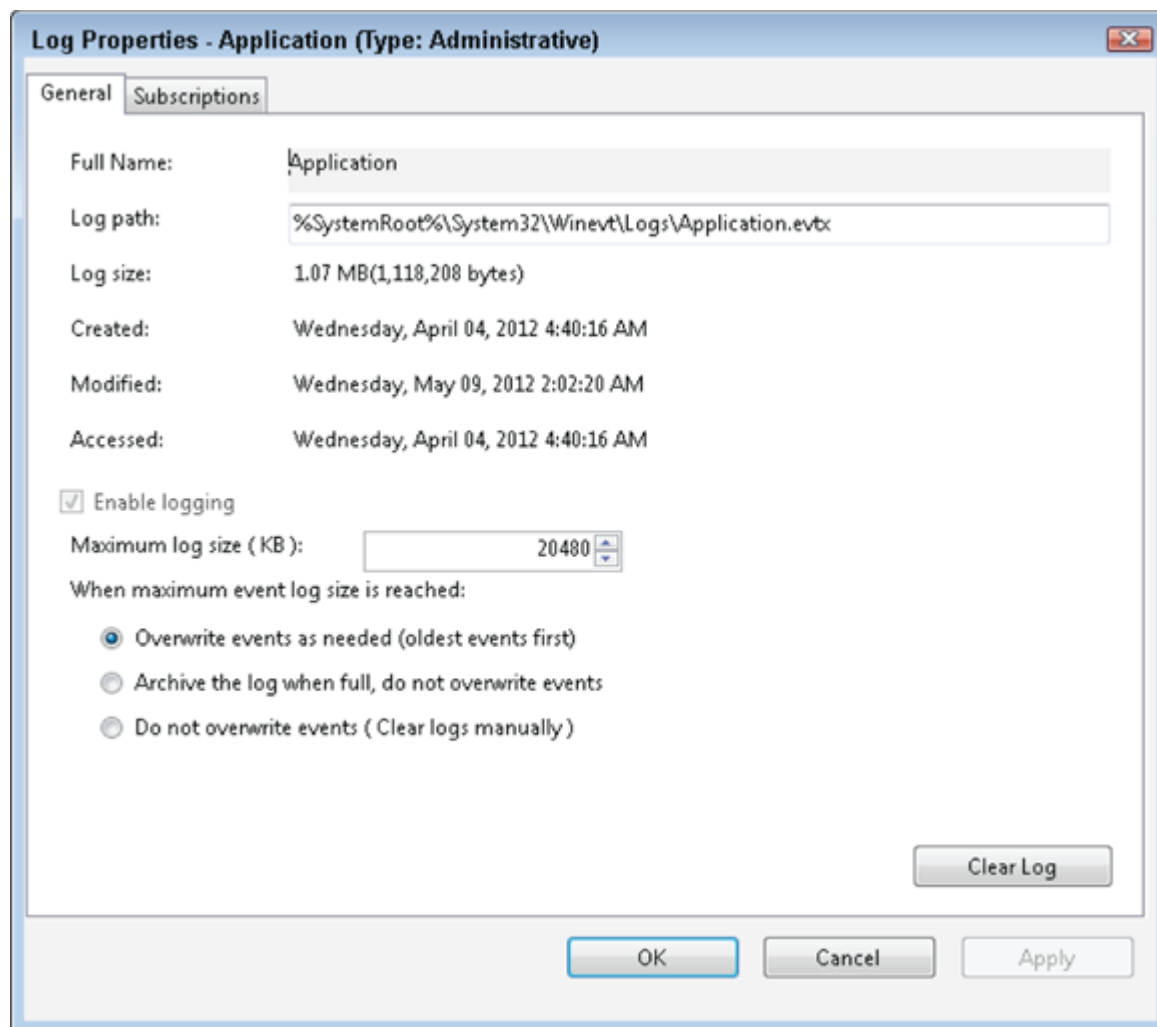


**FIGURE 1-4:** Even with Error Reporting enabled, you can control what errors go to Microsoft.

## *Event Viewer*

Windows offers various logging tools, the greatest of which uses the Event Log service. The Event Log service logs errors and events into several different log files. The Event Viewer is the application you use to view the contents of these log files.

Windows always has at least three default logs: Application, Security, and System. These log files have a default size of 512KB each and automatically overwrite events after seven days in Windows XP and have a default size of 20MB each and automatically overwrite events as needed in Windows. These settings can be adjusted for each file by right-clicking the log file in Event Viewer and choosing Properties to open the Log Properties dialog box, shown in [Figure 1-5](#).



**FIGURE 1-5:** The default settings for the Windows 8.1 and Windows 10- log files will prevent them from filling.

In the event that any log fills up, you receive a pop-up message.

- » On Windows 7 or later, choose Start ⇒ Search, type **Event Viewer**, and press Enter. Then expand Windows Logs in the navigation pane, right-click the log, and choose Clear Log.

When you clear the log, you have the opportunity to save the events to a file.



**TIP**

Before clearing the filled log, examine the most recent events for an error that might have caused the log to fill quickly.

## *Getting an A+*

This chapter examines a number of common errors that you are likely to encounter with Windows computers. These errors range from configuration settings and files to boot files and driver-related problems. You also see some common resolution methods, such as booting into Safe Mode. Some key elements to remember in this chapter are

- » `No operating system found` is an error message that means the computer is unable to find a boot device.
- » Most Windows boot sector or boot file errors can be fixed with either the Emergency Repair Process or Recovery Console.
- » Safe Mode is used to diagnose and resolve driver or startup problems.
- » Event Viewer should always be checked as part of the troubleshooting process to see what error messages are being reported by Windows.

## *Prep Test*

- 1. Which of the following options are valid procedures for trying to resolve corrupted boot files with Windows 7? Choose all that apply.**
  - (A) Recovery Console
  - (B) `winload.exe`
  - (C) `ntoskrnl.exe`
  - (D) Emergency Repair/Startup Repair Process
- 2. Which of the following are loaded when you boot into Safe Mode? Choose all that apply.**

- (A) Base video driver
- (B) Your mouse driver
- (C) Auto-start services
- (D) Enabled device drivers

**3. What is the purpose of a swap file?**

- (A) To prepare files to be copied to other disks
- (B) To act as additional memory for the system
- (C) To act as an extension to the hard drive
- (D) To prepare files that are saved to disk

**4. Where do you go to read and clear the Windows 10 Event Log?**

- (A) Event Log
- (B) Event Viewer
- (C) Log Reader
- (D) Disk Cleanup

**5. Which of the following is the default user profile path in Windows 7?**

- (A) C:\Users
- (B) C:\Windows\System32
- (C) C:\Windows\Config
- (D) C:\Documents and Settings

**6. Which of the following tools can you use to force your Windows 10 system to boot into Safe Mode?**

- (A) PowerShell
- (B) Event Log
- (C) Regedit
- (D) Msconfig

**7. Which of the following is a Linux boot loader?**

- (A) SCSI
- (B) MBR
- (C) GRUB
- (D) NTDETECT

**8. When should you boot into Safe Mode?**

- (A) At every boot-up
- (B) When your system will not boot normally
- (C) When your computer is connected to the Internet
- (D) Only to play Solitaire

## *Answers*

1. **A, D.** Both Recovery Console and the Emergency Repair/Startup Repair Process allow you to repair problems with the boot files. Check out “[Windows Boot Files and Failure-to-Boot Errors.](#)”
2. **B.** A base video driver and your mouse driver are the only items on the list that load when you enter Safe Mode. It also loads a VGA-compatible video driver and a minimal set of device drivers. Peruse “[Safe Mode.](#)”
3. **B.** The Windows swap file acts as additional memory, or virtual memory, for the OS. Take a look at “[Paging file errors.](#)”
4. **B.** Event Viewer is used to read, back up, and clear your event logs. Look over “[Event Viewer.](#)”
5. **A.** Microsoft simplified the user profile path in Windows Vista and beyond, switching from `C:\Documents and Settings` to the easier-to-type `C:\Users`. Review “[Registry corruption.](#)”
6. **D.** You use the System Configuration (msconfig) utility to adjust various startup options on Windows Vista, Windows 7, Windows 8.1, or Windows 10 computers. Look at “[Safe Mode.](#)”

7. **C.** GRUB is the most common bootloader found in Linux distributions today. Read “[\*Solving Linux Boot Issues\*](#).”
8. **B.** You should enter Safe Mode to correct problems when your computer won't boot normally. See “[\*Safe Mode\*](#).”

## Chapter 2

# Managing Common Problems

---

### IN THIS CHAPTER

- » Recognizing and resolving Windows service problems
  - » Identifying and correcting auto-restart and blue screen errors and system lockup problems
  - » Knowing and fixing device driver failures
  - » Resolving issues with missing DLL files
  - » Distinguishing and rectifying application install, start, and load failures
- 

In this chapter, you examine some common errors that you will encounter when servicing computers. I show you how to gather the information that you need to properly diagnose and correct the problem. You also look at several common errors and problems that you are likely to encounter when dealing with Windows-based systems.

And because these are some of the most common problems that you will run into at the OS level as a CompTIA A+ Certified Professional, this chapter prepares you for these problems, and will help you on the A+ exams.

## *Solving Windows-Specific Service Problems*

Many jobs are performed on your Windows computer by services. Services are programs that operate in the background, typically programs without a user interface or windows. Most of the time, services will tick away in the background doing their jobs without an issue; but at times,

they stop doing their job. A service is a program and is really no different from any other program; it may have programming flaws and may crash or stop responding. As an example, in this section, you take a look at the print spooler service.

Prior to print spooling being integrated with an OS, the application that was printing had to send each piece of data to the printer, halting the user from doing anything until the printing process was complete. A print spooler is used to quickly accept print data from the application, allowing control of the application to be returned to the user after a very brief spooling process. When the spooler takes the print data from the application, it stores the data in a temporary file, until the spooler has time to send the data out to the printer, or de-spool the data.

From time to time, when dealing with Windows, you can encounter a stalled print spooler. This seems to be a feature of the print spooler service. After a period of printing, and printing well, the print spooler decides to stop responding to further commands. This has been a long-running issue for Microsoft, but seems to happen less frequently with newer versions of the Windows OS. Although the print spooler service seems to be better behaved these days, other services on your computer may not be as well behaved.

When a service stops performing its job properly, the symptoms can vary. You can identify a stalled print spooler service from the following:

- » Users cannot add new jobs to the print queue.
- » Nobody can remove jobs from the print queue.
- » Existing jobs do not print.
- » The print queue appears empty even though it was sent print jobs.

If the print queue exhibits these symptoms, restart the print queue; for any other service, you can restart that service. Use either of the following methods to restart the spooler service:

- » **The Services MMC snap-in**



In Windows 10, open Start, type `services.msc`, right-click the Services Microsoft Management Console (MMC) search result, and click Run as Administrator. Locate the Print Spooler service in the list of services, right-click it, and choose Restart (as shown in [Figure 2-1](#)). You could also choose to Stop, wait for that action to complete, and then choose Start.

## » The `net` command

From the command prompt, use

```
net stop spooler  
net start spooler
```

or

```
net stop "print spooler"  
net start "print spooler"
```



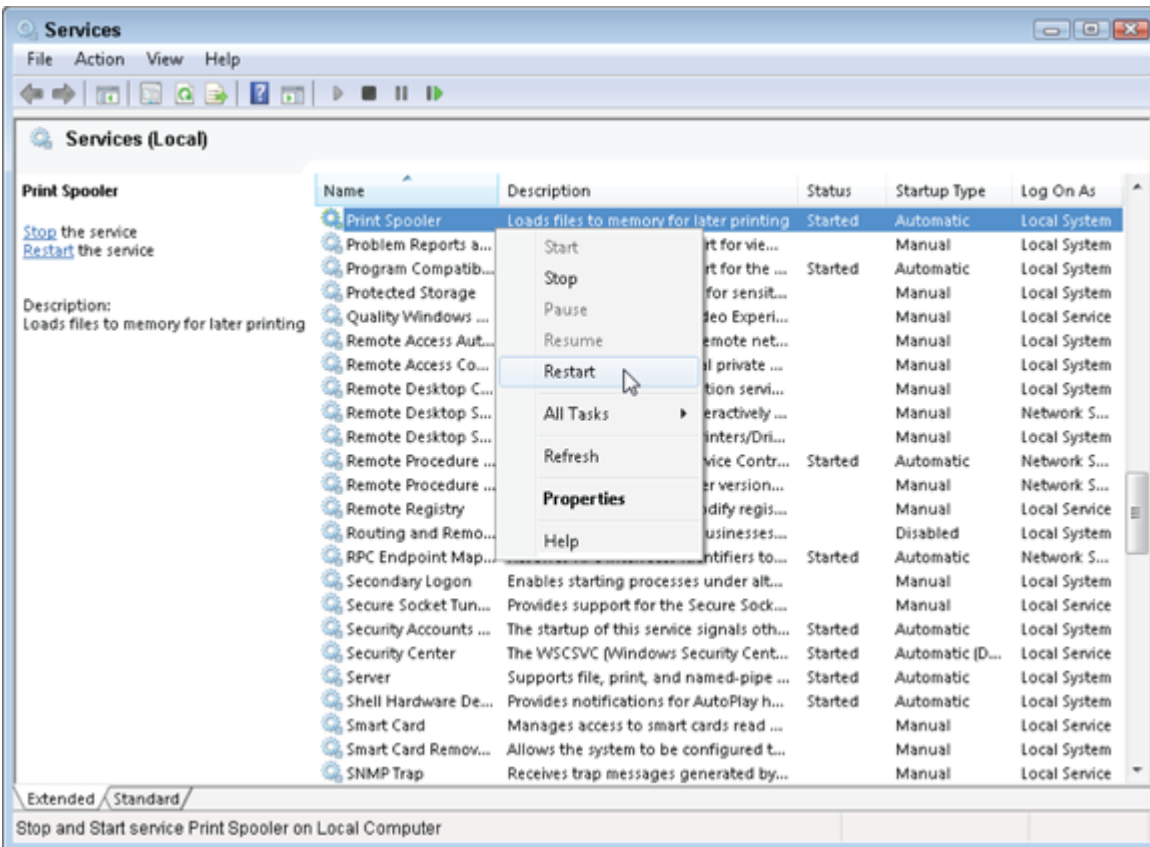
**TIP**

If you don't know the name of the service you want to start or stop, use `net start`, and Windows lists the registered services.



**FOR THE  
EXAM**

If your print spooler is suffering from any problem, restarting the spooler service is usually the correct answer.



**FIGURE 2-1:** Restarting services is easy from the Services Administrative tool.



**ON THE  
WEB**

Lab 2-1 provides practice restarting the print spooler via the command prompt. This lab requires a Windows computer. The labs can be downloaded from the companion website at [www.dummies.com/go/aplusaio](http://www.dummies.com/go/aplusaio).

After the service restarts, your problems should be gone.

## ***Solving Boot Errors and Errors Requiring Restarting***

With the number of computers in most offices and how the law of averages works, it seems like there is always a problem that requires or

causes a reboot. In large offices, it can seem like the Welcome to Windows chime is always playing. In fact, so many support people have used rebooting as the first step in dealing with problems that some users now instinctively reboot even before calling in a support person. This is not always the best course of action because it often removes information that can be used to locate the root of the problem.

## *Auto-restart errors*

In many cases, auto-restart errors are caused by power-related issues, other hardware failures, or software configuration problems. If the computer auto-restarts, something is definitely wrong.

Some common issues that can cause auto-restarts include

- » **Service configuration:** When configuring Services, you can choose an action to be taken when the Service fails. One action is to restart the computer. If you have a Service that is failing and it is configured to restart the computer when it fails, this causes an auto-restart. This setting can be seen in [Figure 2-2](#). More information on Services can be found in Book 6, [Chapter 3](#).
- » **CPU fan:** Most computers have a default thermal setting for the computer to cause a temporary shutdown. If the CPU fan fails, the CPU's temperature quickly rises to where the motherboard interrupts the power to prevent damage to the CPU. Dust caked in and around the heat sink and fan has the same effect. A visual inspection of the CPU fan will show you whether it is running, or whether dirt or debris are the culprits. Book 4, [Chapter 1](#) talks about ventilation methods as well as problems related to poor ventilation.
- » **Power supply problem:** Power supplies have limited life spans. When they fail, their demise is often complete and immediate. In some cases, they can supply some power for a period of time, but as they heat up, they cause an interruption in the power, thus restarting the computer. It is easier to diagnose a complete failure of the power supply rather than a power supply that fails when it is hot because for the latter, you need the power supply operating for a period of time — possibly days — before you see the problem. When in doubt, swap it

out. Power supplies are not expensive and are easy to replace — and if it fixes the problem, you will know it quickly. For more on power supplies, see Book 2, [Chapter 6](#).

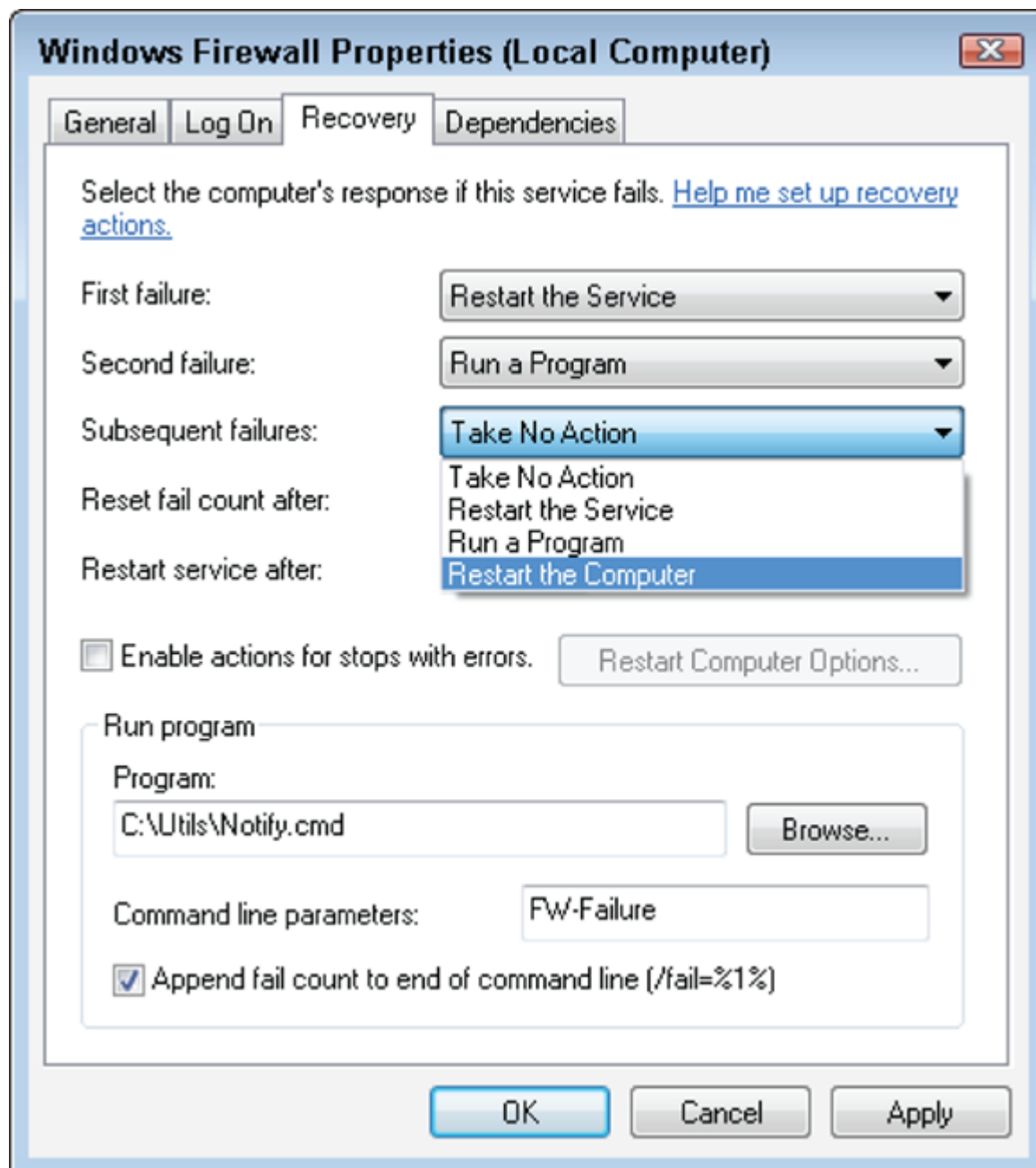
- » **Power source problem:** Some buildings are notorious for power spikes or drops. In some cases, the power can drop to a point that there is insufficient power for the computer, even though other electrical devices do not show any signs. If this problem happens regularly, it will likely affect a number of computers.

Choose from a variety of tools for testing the quality of the power coming from the wall. Some low-end, single-computer uninterruptible power supply (UPS) systems give you a display of the current voltage and provide line conditioning on a 120V line, down to 89V. The UPS can also supply some power when the voltage drops below that level. For more on power sources, see Book 2, [Chapter 6](#).

- » **Bad memory:** When memory is the problem (the computer's, not yours), you might see the system running fine until the damaged or bad blocks of memory are used. At that time, the system spontaneously reboots itself or generates a Windows Stop error. Testing tools are available to test for bad memory, so this situation should be easy to diagnose after letting the system run with the testing software working through the blocks of memory. Of course, as the size of the system memory increases, so does the length of time that it takes to test it.
- » **Network attack:** The TCP/IP network stack is very complex, and with Services running over the stack, many software systems can have flaws. Many network attacks performed on Windows systems cause various buffer overflows, which then cause the system to reboot. Worms like Code Red (2001) and SQL Slammer (2003) fall into this category. Freeware tools like Microsoft's TCPView can be used to view current Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) network activity on a computer, which can in turn be used to identify network attacks or problems. It is beneficial to learn how these tools work when you are not experiencing a problem because it will make it easier to identify nonstandard traffic. In most cases, keeping your system up to date on security patches and

virus definitions offers a high level of protection. The only sure protection from network attacks is to not be connected to the network. For more information about network security, read through [Book 9](#).

» **Automatic Updates:** If your system is configured for Automatic Updates from the Microsoft Update website, you might find that your computer reboots while you are not there. If the computer is configured to install updates in the middle of the night, you might see the next morning that it rebooted. Usually, there are warning messages leading up to the reboot although you might not be there to see them. To solve this issue, check the Windows Event Logs and the settings on Automatic Updates in the Control Panel. As part of the Windows Security Center, Windows suggests enabling Automatic Updates. Book 9, [Chapter 3](#) has more information on the Microsoft Update process.



**FIGURE 2-2:** Auto-restarting a service after a failure is just one of the options.

Unexpected reboots can happen for other reasons, but the preceding list describes the most common.



FOR THE  
EXAM

Automatic reboots of a system can have a variety of causes; make sure to be familiar with the list of the most common reasons.

## *Blue screen errors*

Blue screen errors (shown in [Figure 2-3](#)) are almost always related to driver, DLL, or configuration errors. As some people call them, “Blue Screen of Death,” or BSOD, errors are officially Stop errors. In many cases, these will be related to a recent driver change prior to the last reboot. If this is the case, try booting to the Last Known Good Configuration, which will restore the system configuration to the state it was in during the previous reboot. For more information about booting to the Last Known Good Configuration, see Book 7, [Chapter 3](#).

```
A problem has been detected and windows has been shut down to prevent damage
to your computer.
```

```
If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:
```

```
Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any windows updates you might need.
```

```
If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.
```

```
Technical information:
```

```
*** STOP: 0x69696969 (0x00000000,0x00000000,0x00000000,0x00000000)
```

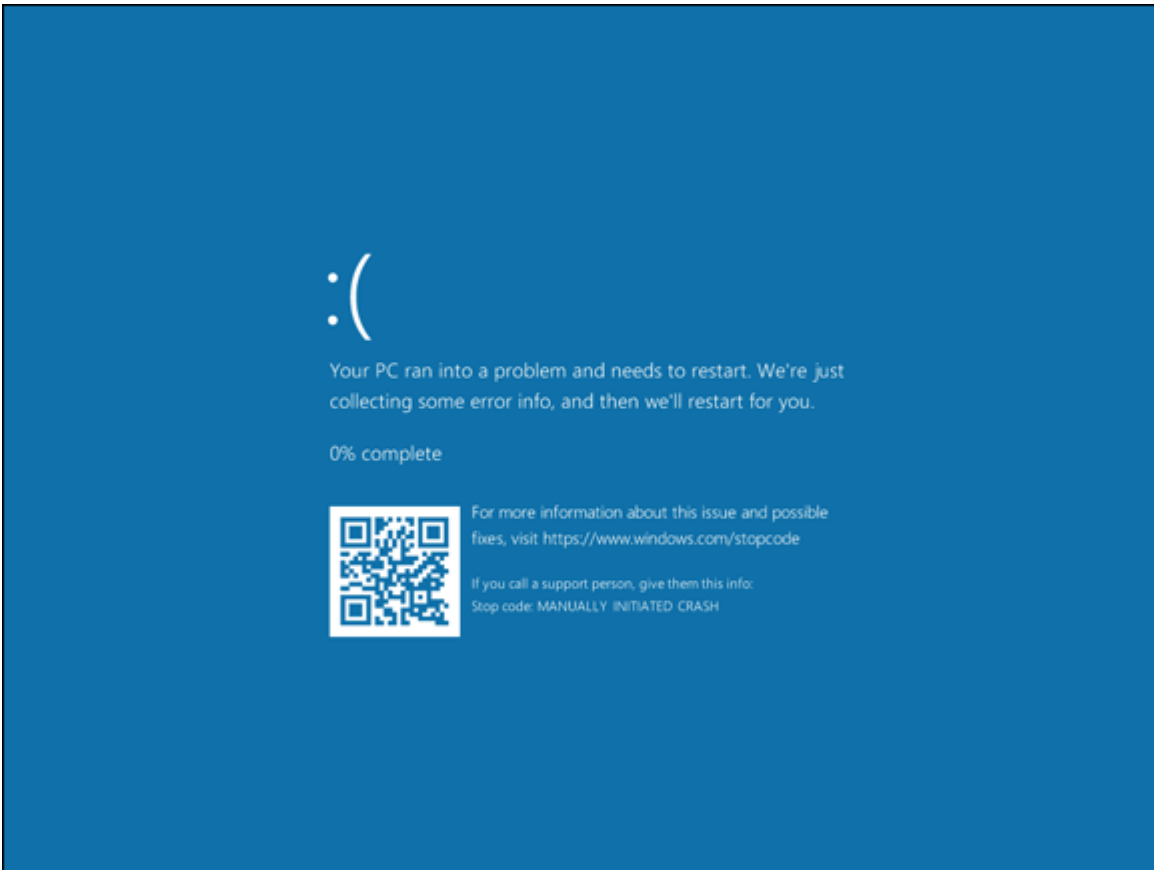
```
Beginning dump of physical memory
```

```
Physical memory dump complete.
```

```
Contact your system administrator or technical support group for further
assistance.
```

**FIGURE 2-3:** Stop errors are “affectionately” known as the Blue Screen of Death.

As you can see in [Figure 2-4](#), Windows 10 presents a less frightening blue screen, complete with an emoticon and a quick response (QR) code you can snap with your smartphone to get more information as to the error's source.



**FIGURE 2-4:** Windows 10 gives you a 21st century, emoticon-friendly stop message.

The most common reasons for Stop errors are

- » Service, application, or device errors
- » Compatibility problems
- » Hardware problems
- » File system corruption or errors
- » Compatibility issues with BIOS/UEFI firmware
- » Viruses



Stop errors occur when one driver or application attempts to access the memory used by another driver. Because drivers operate in the unprotected kernel memory space, this is very bad for system stability. When this happens, Windows does the only thing that it can think of to prevent further corruption — it stops everything. Because applications run in protected memory spaces, they cannot write to memory being used by another application. Thus, Stop errors are caused only by access attempts in the kernel memory space.

The image referenced in [Figure 2-3](#) is a Stop error caused by an application, and the format of the text on the screen is not the same as the Stop error you might be more familiar with, which I discuss later in this section. Alternatively, the first two lines of the Stop error message tell you the name of one of the drivers involved, or at least the memory locations involved.

[Listing 2-1](#) shows text that might appear on a standard Stop error:

### **LISTING 2-1 Sample Stop Error Message**

---

```
*** STOP: 0x0000000A (0x802aa502, 0x00000002, 0x00000D00, 0xFA84001C)
IRQL_NOT_LESS_OR_EQUAL*** Address fa84001c has base fa840000 - ndis.SYS
CPUID: GenuineIntel 5.2.c irql:1f SYSVER 0xF0000565
Dll Base Date Stamp - Name Dll Base Date Stamp - Name
80100000 2be154c9 - ntoskrnl.exe 80400000 2bc153b0 - hal.dll
80200000 2bd49628 - ncrc710.sys 8025c000 2bd49688 - SCSIPIRT.SYS
...
Address dword dump Build [1381] - Name
fe9cdaec fa84003c fa84003c 00000000 00000000 80149905 - ndis.SYS
fe9cdaf8 8025dfe0 8025dfe0 ff8e6b8c 80129c2c ff8e6b94 - SCSIPIRT.SYS
fe9cdb10 8013e53a 8013e53a ff8e6b94 ff8e6f60 ff8e6b94 - ntoskrnl.exe
...
```

Hexadecimal (the Base 16 number system) is used to display all error codes and memory addresses on the Stop error. The first line tells you the error type numerically (0x0000000A), then the memory address of the code that was attempted to be accessed (0x802aa502), the type of access attempted or error parameter (0x00000002, 0x00000D00), and the memory address that made the access attempt (0xFA84001C). This is followed by a line providing you with a text-based description of the

error and, if possible, the name of the driver that was found at that location. This driver might be the one that caused the error or the target of the error. After these lines is a section that lists the drivers found in the memory spaces near where the error occurred, then a section listing memory information for some of those memory spaces. If the error was a result of a recent change to the system, undo that change or update your drivers.

Some common Stop errors you may encounter are

```
» 0x0000000A IRQL_NOT_LESS_EQUAL
» 0x0000001E KMODE_EXCEPTION_NOT_HANDLED
» 0x00000024 NTFS_FILE_SYSTEM
» 0x0000002E DATA_BUS_ERROR
» 0x00000050 PAGE_FAULT_IN_NONPAGED_AREA
» 0x0000007B INACCESSIBLE_BOOT_DEVICE
» 0x0000007F UNEXPECTED_KERNEL_MODE_TRAP
» 0xC000021A STATUS_SYSTEM_PROCESS_TERMINATED
```



**FOR THE  
EXAM**

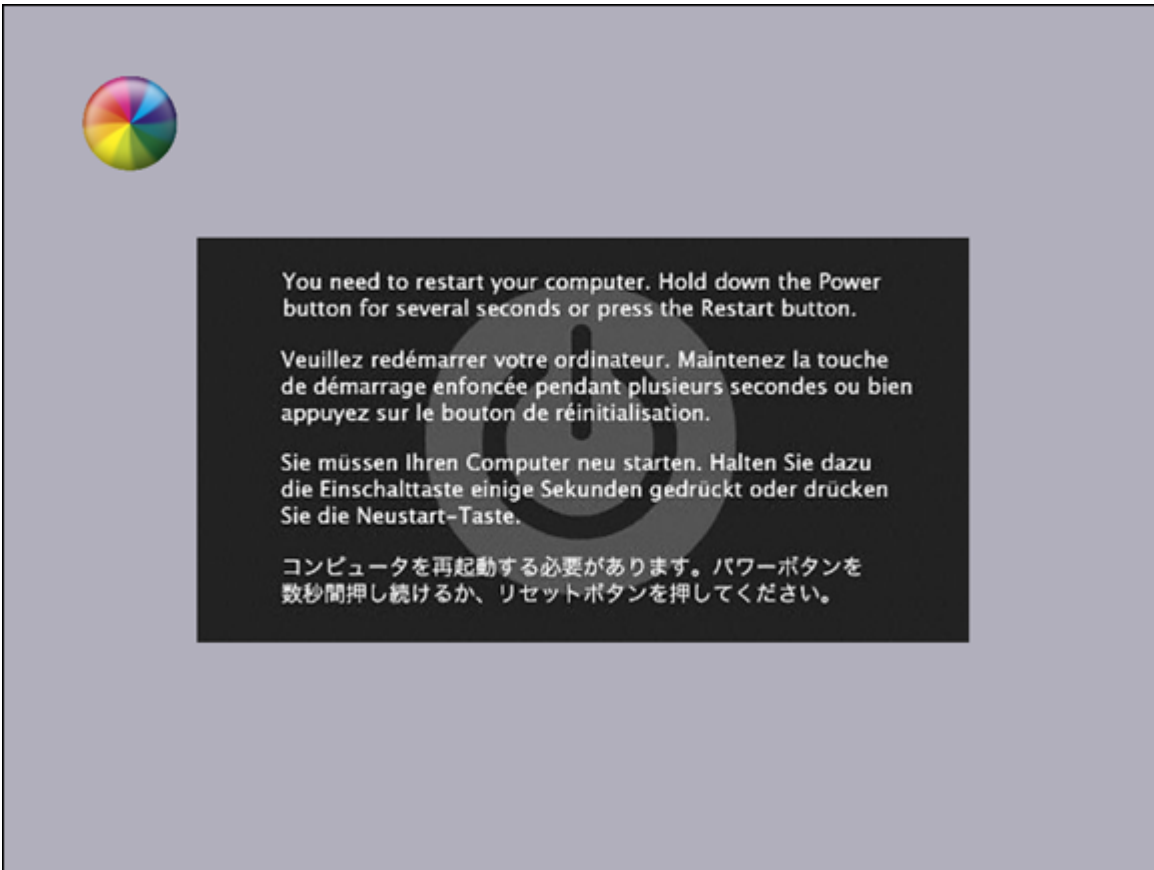
Be familiar with the basic type of information returned in Stop messages.

## ***Proprietary crash screens***

The so-called “Blue Screen of Death” is proprietary to the Windows operating system family. CompTIA also wants you to recognize system crashes on Apple macOS computers.

The “Spinning Beach Ball of Death” occurs when macOS gets stuck due to an application or operating system-level problem, and the mouse pointer turns into a revolving, multi-colored ball icon.

The macOS crash screen (called a “kernel panic message” in Apple documentation) is multilanguage and quite a bit more eye-friendly than the BSOD. I show you a composite of the spinning beach ball of death and the kernel panic screen in [Figure 2-5](#).



**FIGURE 2-5:** The “Spinning Beach Ball of Death” and the kernel panic (system crash) screen in Apple macOS.

## *Blank screen on boot*

When you boot your computer, at times you may find that you are looking at a blank screen. That may cause you to say, “What could be causing that?” Here is a short list of things that you can check:

- » **If you do not see anything from the start of the POST:** Ensure that your monitor is powered up and check all your video connections. If they are good, you could be looking at a bad video card, a defective monitor, or a completely dead computer. If this is a networked computer, verify whether the computer has completed its boot process

and is visible on the network. If it is on the network, this is a video problem.

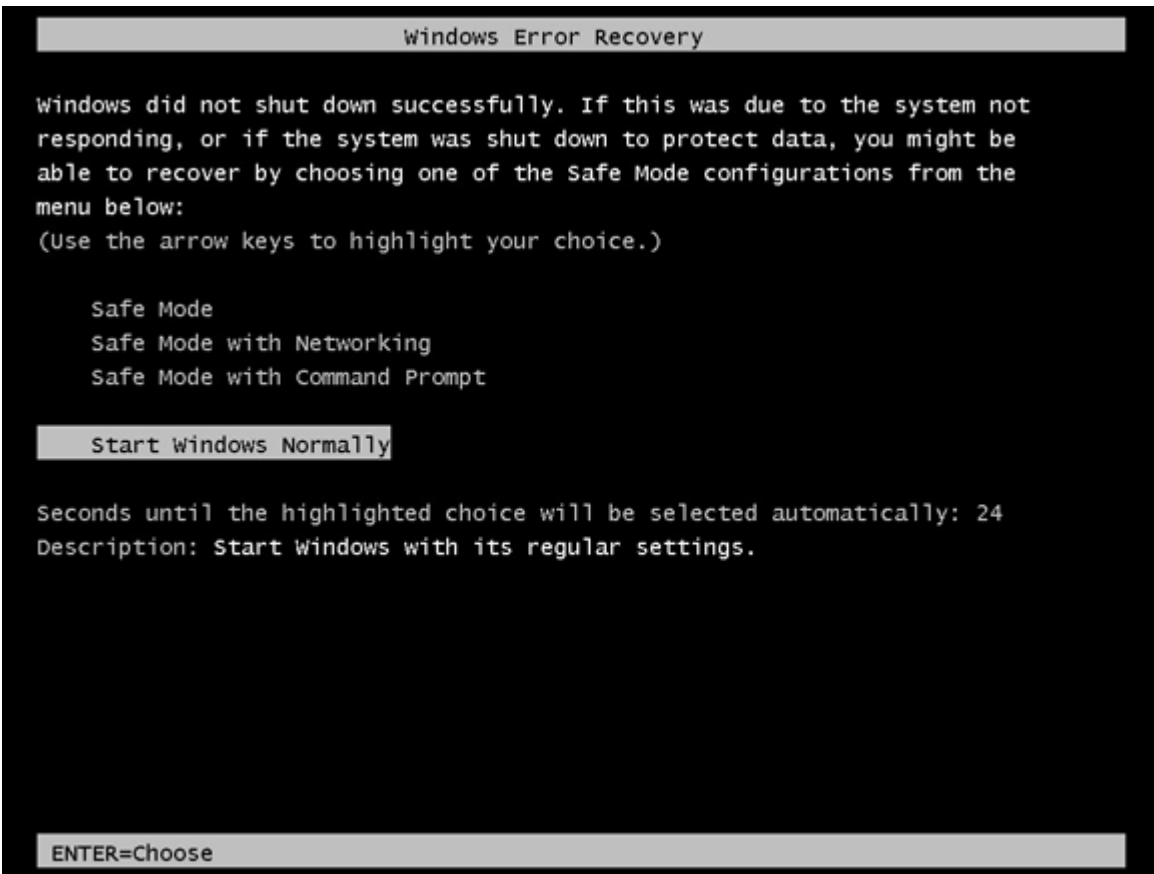
- » **If you see POST information and then lose your video during the boot process**, you know that your hardware is working; rather, you have an issue with the driver or screen resolution. Try booting to Safe Mode, which can use basic drivers and lower screen resolutions. From there, you should be able to adjust the resolution or change the driver that will be used on the next boot.

## *System lockup and improper shutdowns*

System lockup happens when your computer stops responding to any system functions or user input. If you are using Windows 7 or later, system lockups should be rare compared with older OSes, such as Windows XP or Vista. More likely, you will have a period of slow responsiveness. If you are using older Windows OSes, you are likely to have complete system lockups. This has to do with how the operating systems work.

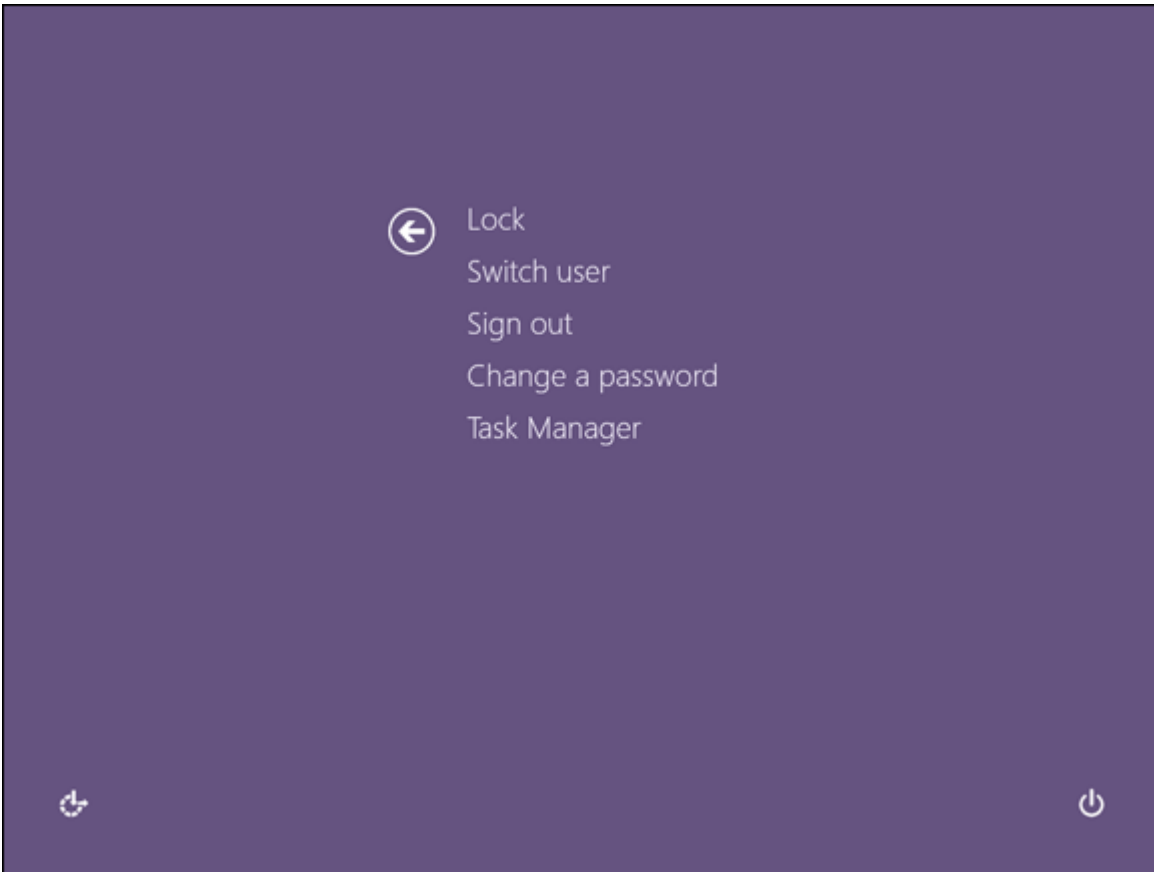
An improper shutdown occurs when you shut down or restart a computer by unplugging the device or by using the hard power switch on the chassis. Doing this is a bad idea for many reasons, not the least of which is that the operating system doesn't have the time to gracefully release memory, store data to disk, and so forth.

Later Windows versions (Windows 8.1 and Windows 10 specifically) will likely boot automatically into the Windows Error Recovery environment, shown in [Figure 2-6](#), if it detects that the system was not shut down gracefully. From here you can launch a startup repair, boot into Safe Mode, or continue a normal boot.



**FIGURE 2-6:** You'll see the Windows Error Recovery screen if your system was shut down improperly.

If you are using Windows 7 or newer Windows OS, you might experience a runaway application or Service that can cause the system to become unresponsive. This unresponsiveness might fool you into believing that your computer is locked up, when in fact it just doesn't have enough clock cycles to pay attention to you. Press Ctrl+Alt+Del to open the security dialog box (shown in [Figure 2-7](#)), where you can launch Task Manager.



**FIGURE 2-7:** Press Ctrl+Alt+Del in Windows 8.1 or Windows 10 to access Task Manager, among other options.

I have seen Windows 7 lock completely up very few times, but there have been many other times when I have powered a machine off because it was slow to respond.

How long you wait for an unresponsive system is typically related to the number of critical unsaved documents that you had open when it became unresponsive. Prior to turning off the computer's power, I have waited an hour to get the dialog boxes to close Microsoft Word and save my documents. Turning off the power (as opposed to performing a graceful shutdown) is usually to be avoided because of the risk of disk corruption. This wait is not typical because in most cases if the system is unresponsive to the point that Task Manager takes more than five minutes to open, I usually press and hold the power button to kill the power to the computer.

The Processes tab of Task Manager (shown in [Figure 2-8](#)) lets you see which application is the runaway. You just have to look for the application with the highest CPU value. This indicates which application is hogging the CPU. You can try to switch to the application and close it normally, but there is a good chance that this will not work. If you cannot shut down the program normally, return to Task Manager, select the task, and click the End Task button. This should return your system to its previous level of responsiveness. In some cases, the application at fault will be a critical system service, like WinLogon, which cannot be stopped, so you will just have to reboot.

Name	Status	11% CPU	13% Memory	4% Disk
<strong>Apps (4)</strong>				
Internet Explorer		0%	65.4 MB	0.1 MB/s
OneNote		0%	13.5 MB	0 MB/s
PC settings		0%	22.1 MB	0 MB/s
Task Manager		4.1%	11.3 MB	0 MB/s
<strong>Background processes (18)</strong>				
Adobe® Flash® Player Utility		0%	2.5 MB	0 MB/s
COM Surrogate		0%	2.2 MB	0 MB/s
COM Surrogate		0%	1.5 MB	0 MB/s
Host Process for Windows Tasks		0%	5.4 MB	0.1 MB/s
Microsoft Distributed Transaction Coordinator Service		0%	1.2 MB	0 MB/s
Microsoft Windows Search Filter Host		0%	1.5 MB	0 MB/s
Microsoft Windows Search Indexer		0%	9.2 MB	0 MB/s
Microsoft Windows Search Protocol Host		0%	1.3 MB	0 MB/s

**FIGURE 2-8:** The Processes tab in the Windows 10 Task Manager enables you to view resource consumption as well as stop stuck programs.

# *Resolving Device Driver and Service Errors*

Other than a system Stop error, device drivers or services might fail to load for a number of reasons:

- » **Version:** The version of the driver or service might not be compatible with the OS version.
- » **Configuration:** The driver or service could be misconfigured, and some settings require changing.
- » **Incompatibility:** The driver or service might not be compatible with some other driver, service, or application running on the system.
- » **Dependency:** The driver or service may be dependent on another driver or service that has not started up.

In most cases, the startup error for the driver will be listed in the Event Viewer error logs. Open Event Viewer from Start by typing **Event Viewer** and clicking the appropriate search result; then click one of the three log files to view the error logs. After locating the error in Event Viewer, you may use other Windows administrative tools, such as Device Manager or Services, to correct the problem. Typically, the long-term fix for these issues involves a visit to the vendor's website and downloading the latest version of the software or reviewing the vendor knowledge base for a fix to the compatibility problem. In rare cases, it might mean changing to a different version of the device or service, possibly from a different manufacturer.

“Missing DLL” messages are always unfortunate, and usually require that you uninstall and re-install the reporting application. What I've found in my experience is that sometimes uninstalling application A removes dynamic link library (DLL) files that application B requires. Thus the error message appears the next time you start application B.



# *Application Install, Start, and Load Failures*

From time to time, you will have applications that will not start. A few reasons for this problem include corrupted or damaged shortcuts, damaged or corrupted settings, missing files, or corrupted memory space. In the following sections, I take a closer look at these three types of errors as well as application installation errors.

## *Corrupted shortcuts*

When you create a shortcut to a program, the shortcut records information about the target file, such as size and creation date. If something happens to the original file, such as being moved to another directory, the shortcut will attempt to search the hard drive and repair the shortcut. In older versions of Windows, you will be prompted to verify that the correct file was found. On Windows Vista and newer OSes, automatic link tracking is enabled on shortcuts. What this means to you is that unless the file was deleted — in which case you will be asked to delete the shortcut — your shortcut links will always work, no matter how much you move a target file.



**TIP**

Do not always choose to delete damaged shortcuts because Windows will report that a file is missing if your files are on a network server but you are disconnected from the network. If you reconnect to the network, your shortcut should work again. In the worst case, you have to re-create the shortcut by hand.

## *Damaged setting*

Applications may store settings in a variety of locations, from the file system to the Windows Registry. If the application is failing to start due to corrupted settings, those settings need to be corrected or removed. The location where you will go to resolve the issue will depend on where the

settings are stored. So, you may need to locate the settings in the Registry, or edit or delete the configuration file that has the settings stored.

### *Missing files or DLLs*

If the computer user has been performing some manual disk cleanup, has been running programs from a server, or has suffered from disk corruption, required files might be missing. Depending on the error handling that the programmer is using, it may report to the user exactly which files are missing from the computer. In any case, if the running program has lost access to the files, this connection to the files needs to be restored. For users running programs from a network server, you may need to follow network troubleshooting processes to restore the network connections. For missing local files, you may need to copy the missing files from another computer with the application installed, or re-install the application.

If the missing files are OS files rather than application files, you should look at the Emergency Repair process, covered in [Chapter 3](#) of this minibook. Alternatively, for missing OS files, you may be required to re-install Windows.

### *Applications will not install*

In some cases, you will find that applications just do not install. This may be caused by the application performing a compatibility test, which your computer fails. If this is the case, you should be notified of the compliance failure by the application. If your computer is less powerful than recommended, it should be upgraded to support the application.

In some cases, specifically with Windows Installer applications, you might not be able to perform an installation if there is a previous installation that is still pending a reboot. The older setup applications might not install if they see another copy of `setup.exe` running. If this copy of setup is not expected to be running, check Task Manager to see whether it is there. Rebooting the system will correct both issues.

### *Services fail to start*

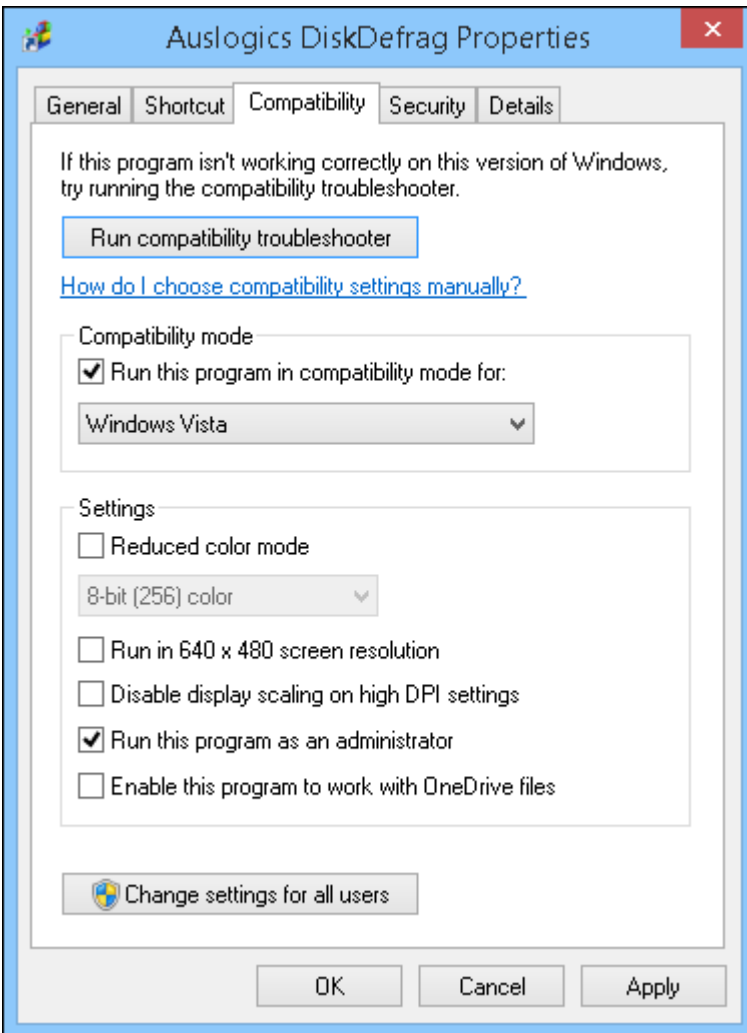
One common reason that some services get “stuck” is that the computer is pending a reboot from a Windows Update process. Try restarting the computer, open the Service Control Manager tool, and verify that the service is now started.

You may also want to inspect the service properties and change the user account under whose credentials the service runs. This is an especially important consideration for services running on Windows Server machines. For example, if a service requires administrative privileges and it’s configured to run in the security context of a standard user, then that service simply won’t behave correctly.

### ***Compatibility errors***

Modern Windows versions include a compatibility subsystem in which you can “trick” a troublesome application into “thinking” it’s running in a previous Windows version.

As you can see in [Figure 2-9](#), right-clicking an application shortcut and navigating to the Compatibility tab gives you the relevant options.



**FIGURE 2-9:** You can run applications in compatibility mode if they don't run correctly in the current Windows version.

In my experience, the application compatibility tools that are built into Windows 7, Windows 8.1, and Windows 10 are functional enough for casual situations (trying to run a retro game, for example). However, you should know that in the enterprise, most systems administrators turn to application virtualization solutions like Citrix XenApp to run troublesome apps in a compatible environment.

## *Solving Linux File-Related Problems*

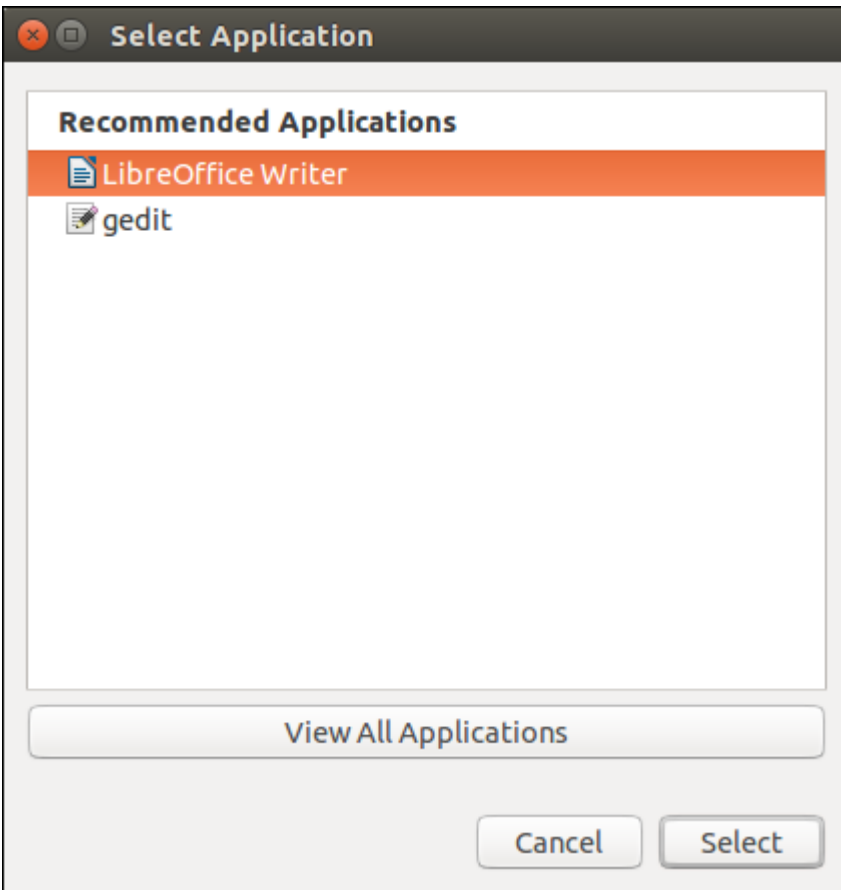
In keeping with CompTIA's recent focus on knowing some Linux and macOS in addition to Windows, let's look at a file-related Linux problem and learn how to solve it.

## *File fails to open*

In Windows, files have a three or more letter extension that is then associated by the operating system with a specific program. For example, Windows will open `.rtf` text files in WordPad unless you specify otherwise.

The same principle applies in Linux, with the exception that file extensions aren't, strictly speaking, required. However, when a file fails to open in Linux, it's amazing how Windows-like the behavior is to resolve the problem.

For example, in Ubuntu Linux's Unity desktop experience you can manually define a file association by right-clicking a file, selecting Open with ⇒ Other Application from the shortcut menu, and choosing the target application in the Select Application dialog box. Easy-peasy! I show you what the interface looks like in [Figure 2-10](#).



**FIGURE 2-10:** You set file associations in Ubuntu the same way you do so in Windows.

## *Solving Other Problems*

In addition to the problems already discussed in this chapter, a number of other things may go wrong. In the following sections, I examine some of those problems.

### *Spontaneous system restart/shutdown*

In my experience, spontaneous system shutdowns and/or restarts are due to one of two factors: temperature or incompatible hardware. If you put your computer on a carpeted floor or against a desk or wall, you may block access vents in the computer's chassis and produce unsafe operating temperatures for internal components. Similarly, if one of your case fans stops working, airflow will be reduced and temperatures will rise.

Computer motherboards have “failsafe” circuitry that simply shuts down the entire board when unsafe temperatures are detected. Therefore, you should include regular case inspections and “dust outs” to your hardware maintenance routines. Modern UEFI firmware often uses sensors to read and report on motherboard component temperatures. You can see an example of a modern UEFI/BIOS interface in [Figure 2-11](#).



**FIGURE 2-11:** Modern UEFI systems normally include rich diagnostics to help you ensure the computer’s operating temperatures are safe.

## *Device will not function*

In addition to configuring the hardware support for system devices, you also have to load the appropriate driver for the device. For Windows 7 and Windows 10, this can be done through Add New Hardware or Add a Device in the Control Panel/Windows 10 Settings pane, respectively. Of course, Windows Plug and Play is normally more than happy to provide you with a device driver.

That said, however, I find that installing a driver from the manufacturer's own website leads to greater device functionality. Later versions of Windows, like Windows 7 through Windows 10, rely heavily on Microsoft Update to locate and install the correct drivers for your devices. For more information about installing devices on your computer, see Book 6, [Chapter 1](#).

## *Multiple monitor issues*

Do you use two or more monitors in your work? I have done so for the past decade, and feel far less productive when I'm forced to use a single-monitor system. Nowadays Windows plays really well with multiple monitors. The key to solving misalignment or orientation issues is to (a) open the Display Control Panel, and (b) specify display properties on a per-monitor basis.

Speaking of drivers, it's especially important in multi-monitor setups to use the manufacturer's device drivers for your video card(s). By doing so you maximize your chances of choosing a compatible resolution and color depth for each display.

## *Getting an A+*

This chapter goes over some problems that computer support personnel typically encounter. The problems include

- » Dealing with stalled print spooler and other services by restarting services
- » Identifying root causes for auto-restart and Stop errors
- » Using Event Viewer to diagnose driver problems
- » Dealing with application start problems in the form of shortcuts, settings, or memory space issues

## *Prep Test*



- 1. When the print queue on your Windows 10 computer is unresponsive, what should you do first?**
  - (A) Reboot the server.
  - (B) Re-install the printer.
  - (C) Restart the Print Spooler service.
  - (D) Redirect the printer to a remote print device.
  
- 2. What command is used to restart a service from the Windows command prompt?**
  - (A) `service.exe`
  - (B) `services.exe`
  - (C) `cmdrun.exe`
  - (D) `net.exe`
  
- 3. You can recover from a BSOD error by pressing the ESC key. True or False?**
  - (A) True
  - (B) False
  
- 4. What program can be used to terminate programs running on your computer?**
  - (A) Device Manager
  - (B) Computer Administration Console
  - (C) System Information
  - (D) Task Manager

- 5. Your computer has had a Stop error, and the first two lines read**

```
*** STOP: 0x0000000A (0x802aa502, 0x00000002, 0x00000D00, 0xFA84001C)
IRQL_NOT_LESS_OR_EQUAL*** Address fa84001c has base fa840000 - i804prt.SYS
```

**Which of the following statements are true? (Choose all that apply.)**

- (A) The type of error was `IRQL_NOT_LESS_OR_EQUAL`.

- (B) The error is due to the BIOS version.
- (C) The driver `i804prt.sys` was involved in the error.
- (D) The driver `i804prt.sys` is located at memory address `0x802aa502`.

**6. What Windows function keeps your shortcut links from breaking?**

- (A) Link Tracking
- (B) Shortcut Locator Service (SLS)
- (C) System Information
- (D) Task Manager

**7. What tool should you check first when things are not working properly and you suspect an error, but you have not seen an error message?**

- (A) System Information
- (B) WinMSD
- (C) Device Manager
- (D) Event Viewer

**8. During your computer's boot process, your computer reboots automatically. There is no sign of a blue screen error. What are the most likely issues? (Choose all that apply.)**

- (A) Hardware problem with power supply
- (B) Driver issue
- (C) Service configuration
- (D) Memory error

## *Answers*

1. C. Restarting the print spooler service should fix problems with the print queue. If it does not, then you may have to restart the server. *See*

*“Solving Windows-Specific Service Problems.”*

2. **D.** `net.exe` is the command that can stop and start services from the command prompt. Review *“Solving Windows-Specific Service Problems.”*
3. **B.** This is false. A Blue Screen Death (BSOD) error is a full-system halt that is resolved only by restarting the system. See *“Blue screen errors.”*
4. **D.** Task Manager can terminate running applications or background processes. Device Manager can be used to configure hardware devices. System Information can provide status and configuration information about most areas of your computer. *Take a look at “System lockup and improper shutdowns.”*
5. **A, C.** The error is of type `0x0000000A: IRQL_NOT_LESS_OR_EQUAL`. The error involves `i804prt.sys`, which is found at memory address `0xFA840000`, not `0x802aa502`. There is no information suggesting that the problem may involve the system BIOS. *Peek at “Blue screen errors.”*
6. **A.** Link tracking is the OS function that keeps track of the executables that shortcuts refer to. *Look over “Corrupted shortcuts.”*
7. **D.** Event Viewer is one of the first utilities that you should use when trying to find out why your system is not responding correctly. WinMSD is the old term used for the System Information tool. Device Manager would list devices that did not start up correctly but would be unrelated to some errors that your system may experience. *Study “Resolving Device Driver and Service Errors.”*
8. **A, C, D.** The only item that it might not be is a driver issue. Most of the time, if there is a driver issue, the driver will either not start up or will trigger a Stop (blue screen) error. *Refer to “Solving Boot Errors and Errors Requiring Restarting.”*

## Chapter 3

# Preparing for Disasters with Disaster Recovery

---

### IN THIS CHAPTER

- » Booting Windows into special modes
  - » Understanding the Emergency Repair process
  - » Performing backups and restores
- 

Even with the best planning, things go wrong. And when they do, you need to know your options for dealing with the situation. In this chapter, I show you the available options for recovery that are built into the OS. I also introduce you to the concept of a recovery partition and show you how to use a recovery DVD/USB drive.

Small issues that arise can be dealt with on the fly if you know what tools are available. This chapter reviews the tools that you need to know. When a large issue appears, it is critical to have a backup, and know how to restore files from it. This chapter also shows you how to perform both processes.

## *Using F8 Options during Boot-Up*

In Windows versions up to Windows 7, you can access the boot menu by pressing F8 immediately after the POST process. After you open the boot menu, you can choose Safe Mode or Safe Mode with Networking. These operating systems also have a Safe Mode with Command Prompt option that loads `cmd.exe` as your shell application.

When you access the F8 boot menu at system startup, you reveal several advanced boot options, depending on your OS:

- » Safe Mode
- » Safe Mode with Networking
- » Safe Mode with Command Prompt
- » Enable Boot Logging
- » Enable VGA Mode
- » Enable low-resolution video (640x480)
- » Last Known Good Configuration
- » Directory Services Restore Mode
- » Debugging Mode
- » Disable Automatic Restart on System Failure
- » Disable Driver Signature Enforcement

## *Booting into Safe Mode*

If the computer hangs or crashes and reboots during the boot process, you might have a device-related error. If a Windows computer fails to boot properly, and you think that the problem is related to a service or driver that is loading, you might be able to boot the computer into Safe Mode.

Windows 8.1 and Windows 10 have an option called Enable Low-Resolution Video, which loads all system drivers with the exception of the video driver. The idea of this option is that with the exception of having the video settings set wrong, the computer will boot and report that some drivers had failed to load — but, it will boot.

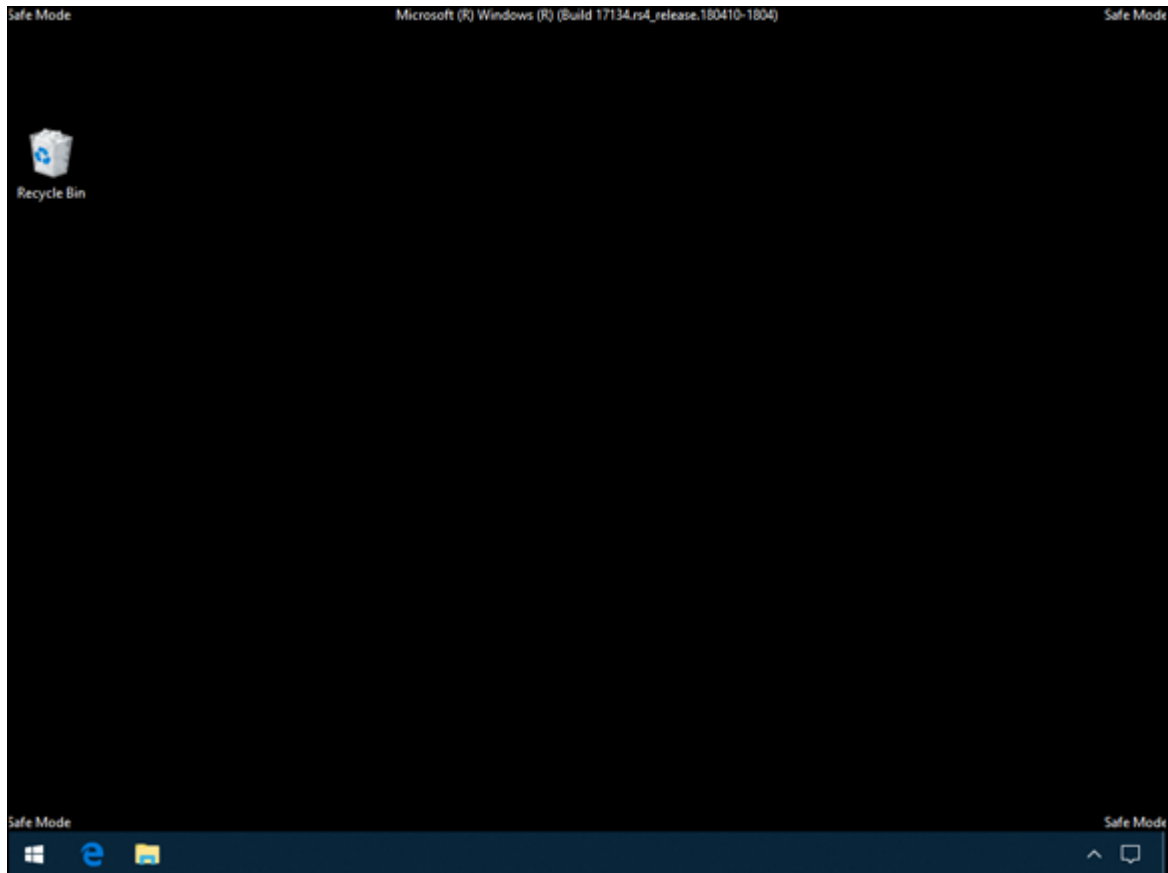


**TIP**

When Windows detects that it failed to boot properly, it may automatically attempt to boot into Safe Mode during the next boot.

When booting into Safe Mode, the OS skips loading any drivers not considered crucial to the boot process. This means that you get a VGA driver providing video in a daring 640-x-480 resolution (16 colors), a keyboard, and a mouse while Windows 7 defaults to 800 x 600, it also

offers a 640-x-480 resolution from Safe Mode. Initially, you will be presented with a warning telling you that you are entering Safe Mode, after which, the words Safe Mode appear in each corner of your screen, as shown in [Figure 3-1](#). Outside of these devices, you will have very few working devices: no sound cards, scanners, or DVD burners. With just the basics running, you should be able to identify the driver that did not load properly and then correct the problem.



**FIGURE 3-1:** Safe Mode should be easy to spot, with the wording in each corner.

Windows also supports an option for Safe Mode with Command Prompt. This mode boots the Windows GUI (graphical user interface) but opens `cmd.exe` as your shell, rather than `explorer.exe`. This allows you to perform many actions to correct your problem (by using utilities such as `chkdsk.exe` or the Registry Editor). When you are done, exiting the Command Prompt reboots your system.

Windows has a boot option for Safe Mode with Networking. This mode is useful when you need to download new drivers for a failed device or access files that might be stored on your server. With the exception of the loading of the networking drivers, this is a standard Safe Mode boot.

## *Tracking the boot with a bootlog*

When choosing the Enable Boot Logging option from the Windows F8 menu, you create a log file called `ntbtlog.txt`, which is saved to the `windows` directory. This file is appended to when performing logged boots.

The `ntbtlog.txt` file is very useful for troubleshooting boot problems. It logs all drivers, services, and resources while they are loading. This file can then be referenced to locate problems with the boot, especially because the system does not give you much indication of what is happening during the boot.

The structure of a `ntbtlog.txt` file from Windows 7 is shown in [Listing 3-1](#). This listing shows two boots of the system, which is noted by the OS identifier line `Microsoft (R) Windows (R) Version 6.1 (Build 7600)`.

### **LISTING 3-1 A Windows 7 ntbtlog.txt File**

---

```
Microsoft (R) Windows (R) Version 6.1 (Build 7600)
5 15 2012 07:29:11.500
Loaded driver \SystemRoot\system32\ntoskrnl.exe
Loaded driver \SystemRoot\system32\hal.dll
Loaded driver \SystemRoot\system32\kdcom.dll
Loaded driver \SystemRoot\system32\mcupdate_AuthenticAMD.dll
<Lines Deleted>
Did not load driver @hal.inf,%acpi_amd64.devicedesc%;ACPI x64-based PC
Did not load driver @mdmgen.inf,%gen556%;Standard 56000 bps Modem
Did not load driver @netavpn.inf,%mp-agilevpn-dispname%;WAN Miniport (IKEv2)
Did not load driver @netrasa.inf,%mp-ip-dispname%;WAN Miniport (IP)
Did not load driver @netrasa.inf,%mp-ipv6-dispname%;WAN Miniport (IPv6)
Did not load driver @netrasa.inf,%mp-pppoe-dispname%;WAN Miniport (PPPOE)
<Lines Deleted>
Loaded driver \SystemRoot\system32\DRIVERS\udfs.sys
```

```
Did not load driver AFD.SYS
Did not load driver AFD.SYS
Microsoft (R) Windows (R) Version 6.1 (Build 7600)
5 15 2012 07:35:01.500
Loaded driver \SystemRoot\system32\ntoskrnl.exe
Loaded driver \SystemRoot\system32\hal.dll
Loaded driver \SystemRoot\system32\kdcom.dll
Loaded driver \SystemRoot\system32\mcupdate_AuthenticAMD.dll
<Lines Deleted>
Loaded driver \SystemRoot\System32\DRIVERS\srp2.sys
Loaded driver \SystemRoot\System32\DRIVERS\srp.sys
Did not load driver \SystemRoot\System32\DRIVERS\srp.sys
Loaded driver \SystemRoot\system32\DRIVERS\asynmac.sys
```

The `ntbtlog.txt` file in [Listing 3-1](#) lists the devices that were loaded and the order in which they were loaded. Look through the listing to see what other drivers or devices you can identify. When checking the file, look for items that list `LoadFailed` or `Did not load driver` because those are failures related to current problems.

## *Using the Last Known Good Configuration*

If you just updated a driver on your Windows computer and your computer will not boot, try booting into Safe Mode to troubleshoot the issue. If the driver update is causing problems with Safe Mode as well, you still have options. Later in this chapter, you can read about the System Image Emergency Repair Process, but in some cases, it is quicker to restore the Last Known Good Configuration.

The `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet` Registry key stores the load or startup settings for all devices and services on your computer, including the path to the driver that is to be used. By choosing to restore the Last Known Good Configuration from the F8 boot menu, you can quickly and automatically restore this section of the Registry with a copy that was used during your last successful boot. If your computer had been running for a long time with many potential changes to this Registry key, those other changes will be lost while you are repairing the boot problem. You will have to decide whether the loss of those other changes is worth the quick restoration of a bootable computer.



## *Other Windows boot options*

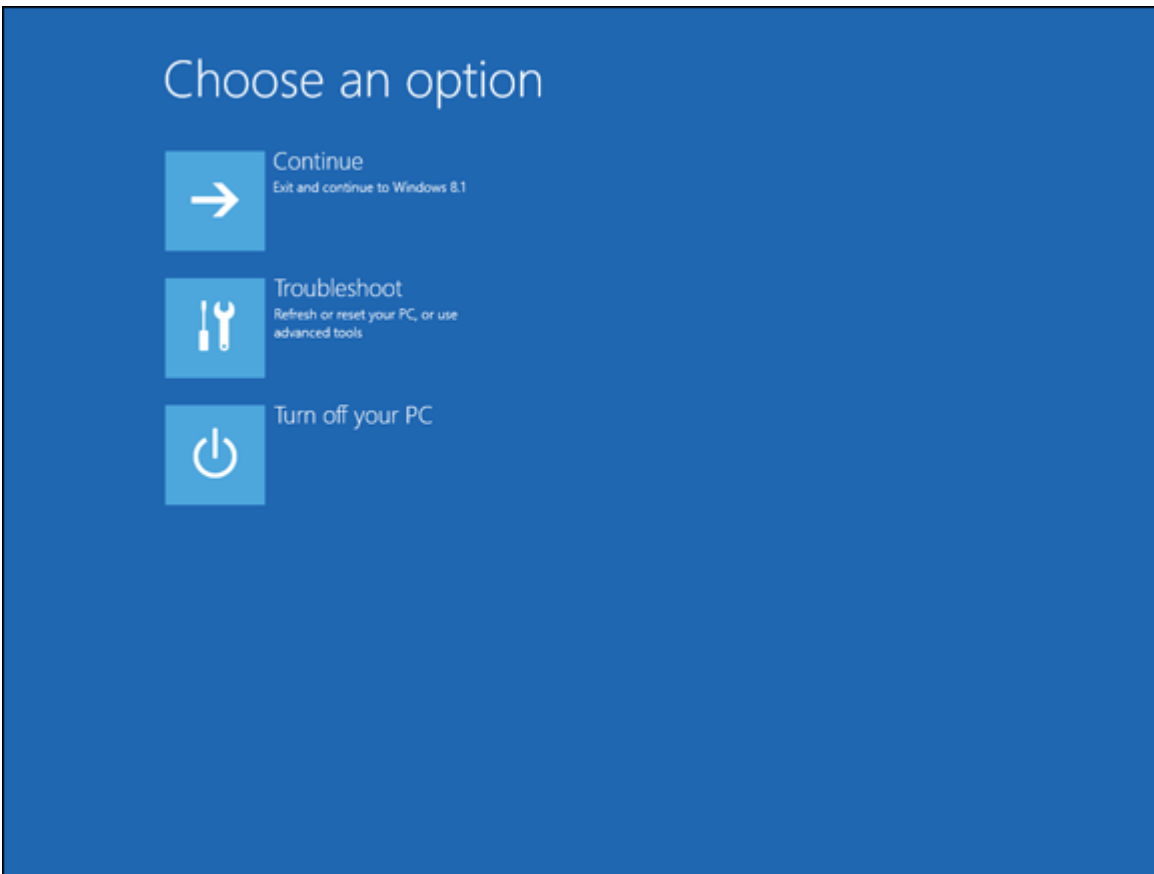
There are a few other advanced boot options for Windows that you will rarely use, so they are briefly covered here:

- » **Directory Services Restore Mode (for Windows Server Domain Controllers):** This boot option will never be used with Windows client computers (even though it is in the Options menu) because it is designed to restore the Active Directory database, which would be running on a Windows Server–based domain controller computer.
- » **Debugging Mode:** This option is for use with external debuggers, which you might be asked to set up during troubleshooting sessions with Microsoft Professional Services after placing a support call.
- » **Disable Automatic Restart on System Failure:** Some drivers may be configured to cause the system to reboot if they fail to load, but this option prevents the system from rebooting. This option is used to allow the system to complete its boot so that you could perform troubleshooting from within the OS.

## *Accessing startup settings in Windows 8.1 and Windows 10*

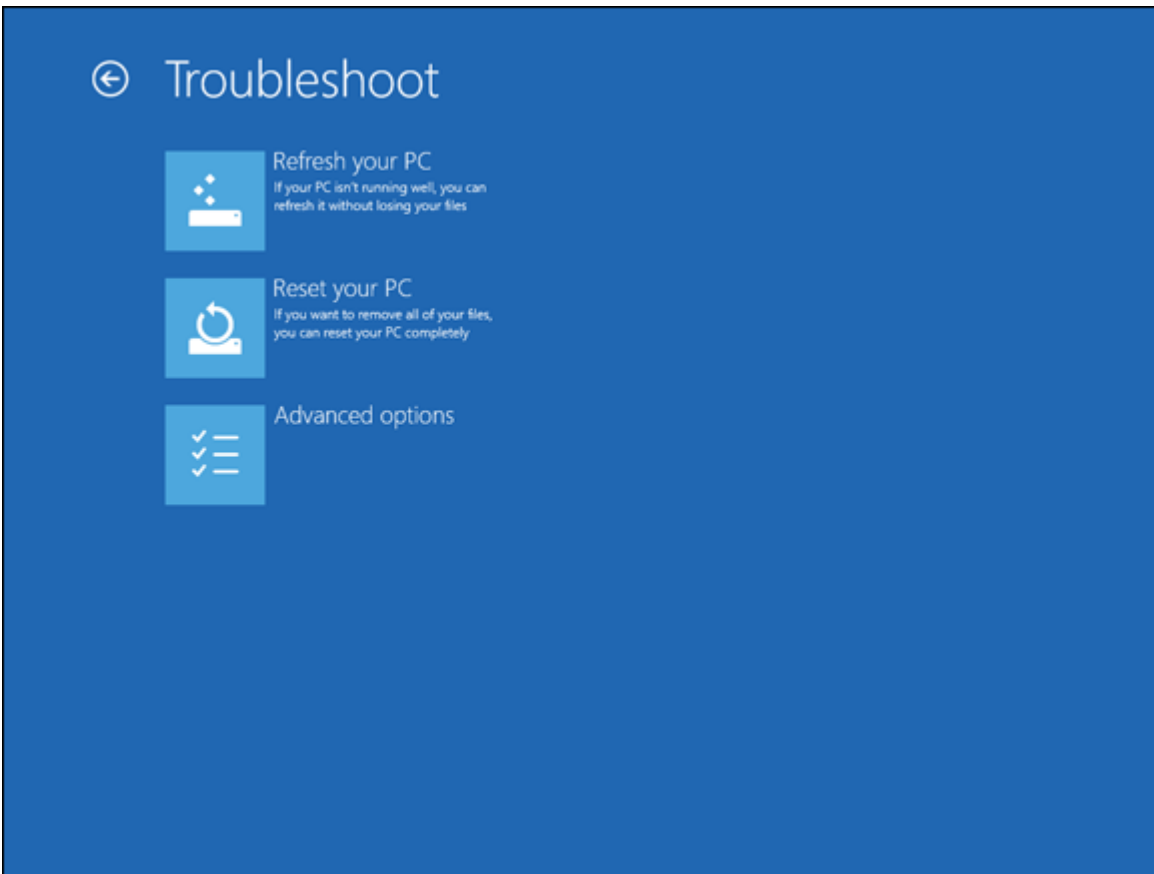
Windows 8.1 completely revamps how system troubleshooting and recovery take place. You now have the Windows Recovery Environment (Windows RE), a graphical shell that gives you access to the mouse, the network, and the local system drive, all from a RAM disk environment.

To reboot a Windows 8.1 or Windows 10 system into Windows RE, open Start, hold down the Shift key, open the Power menu, and select Restart. In a moment you'll be asked to Continue normal boot, enter the Recovery Environment, or turn off the PC. I show you this screen in [Figure 3-2](#).



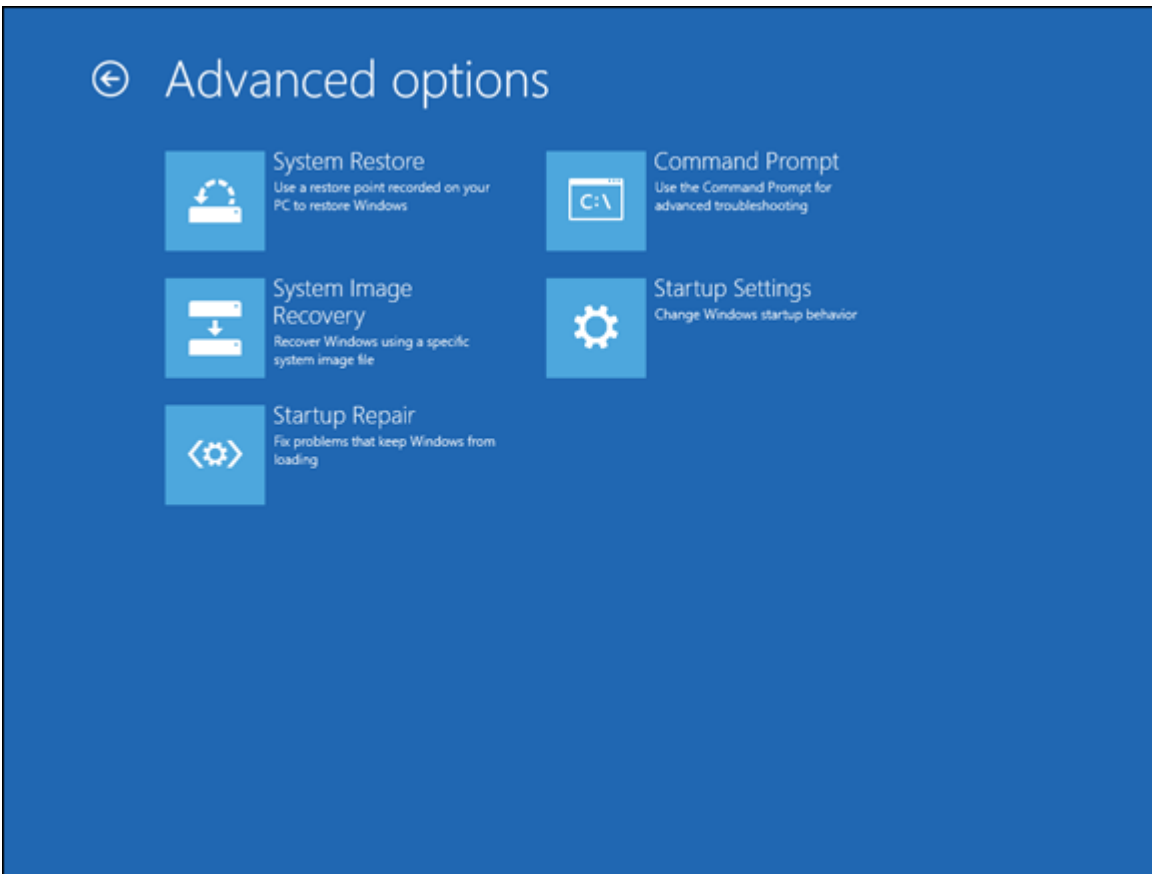
**FIGURE 3-2:** Get ready to enter the Windows Recovery Environment in Windows 10.

In the Choose an Option screen, click Troubleshoot to reach the Troubleshoot screen, shown in [Figure 3-3](#).



**FIGURE 3-3:** Windows RE allows you to refresh, reset, or troubleshoot a Windows 8.1 or Windows 10 system.

Click Advanced Options, and after another short pause you'll reach the Advanced Options screen, shown in [Figure 3-4](#).



**FIGURE 3-4:** The Advanced Options screen gives you access to the core Windows recovery and repair tools.

I discuss the System Restore, System Image Recovery, and Startup Repair options later in this chapter. For now, click Startup Settings to see the aforementioned boot options. This is a much richer interface than users had in Windows 7 and earlier Windows versions, that's for sure!

### *Improper shutdown and boot*

There are times when your computer is not shut down properly. When using Windows, you will be told when the computer is rebooting that there was a problem. When this message appears, it will only remain for 30 seconds and then the default action will be to start Windows normally. The message for Windows 7 is shown in [Listing 3-2](#).

### **LISTING 3-2 Windows Error Recovery for Improper Shutdown**

---

Windows Error Recovery

Windows did not shut down successfully. If this was due to the system not responding, or if the system was shut down to protect data, you might be able to recover by choosing one of the Safe Mode configurations from the menu below:

(Use the arrow keys to highlight your choice.)

Safe Mode

Safe Mode with Networking

Safe Mode with Command Prompt

Start Windows Normally

Description: Start Windows with its regular settings.

Enter=Choose

In the default configuration, a failed shutdown will result in a 30-second delay on the next reboot, but if there is an actual problem, then successive failures will briefly present this message to the user of the computer. This message is displayed to give users an easy way to get into Safe Mode, where they would be able to perform some additional diagnostics to determine why the computer is not shutting down properly.

These messages are a little different from the messages that you will receive if the computer fails to boot up properly, which varies slightly from version to version in Windows Vista, Windows 7, Windows 8.1, or Windows 10. The Windows Vista message conveys the information found in [Listing 3-3](#), which is that something has gone wrong and that you may need your OS installation DVD to repair the problem. Since boot problems are often the result of recent changes, you are also given the option of booting the Last Known Good Configuration from this menu. The default action for this menu is to boot Windows normally.

### **LISTING 3-3 Windows Vista Failure to Boot Recovery Message**

---

Windows Error Recovery

Windows failed to start. A recent hardware or software change might be the cause. To fix the problem:

1. Insert your Windows installation disc and restart your computer.
2. Choose your language settings, and then click "Next."
3. Click "Repair your computer."

Other options:

```
If power was interrupted during startup, choose Start Windows Normally.
(Use the arrow keys to highlight your choice.)
Safe Mode
Safe Mode with Networking
Safe Mode with Command Prompt
Last Known Good Configuration (advanced)
Start Windows Normally
Description: Start Windows with its regular settings.
Enter=Choose
```

The similar message for Windows 7, Windows 8.1, and Windows 10 is shown in [Listing 3-4](#), which also states that the problem may have been caused by recent changes. Rather than showing the standard Safe Mode options, Windows 7 offers you the choice of using the Startup Repair tool to perform startup troubleshooting. The default action for this menu is to launch Startup Repair.

### **LISTING 3-4 Windows 10 Failure to Boot Recovery Message**

---

```
Windows Error Recovery
Windows failed to start. A recent hardware or software change might be the
cause.
If Windows files have been damaged or configured incorrectly, Startup Repair
can help diagnose and fix the problem. If power was interrupted during
startup, choose Start Windows Normally.
(Use the arrow keys to highlight your choice.)
Launch Startup Repair (recommended)
Start Windows Normally
Seconds until highlighted choice will be selected automatically: 30
Description: Fix problems that are preventing Windows from starting
Enter=Choose
```

## ***Emergency Repair***

When things go wrong with the boot of Windows, you can try booting into Safe Mode to repair the error, but sometimes the system will not boot at all. At these times, you can make a final attempt to resurrect the system or start the installation. If you choose to attempt the Emergency Repair

Process, you should be familiar with what options are available. Here I focus on Windows 8.1 because Microsoft put so much effort into its emergency repair tools.

### *Factory repair partition*

That's right — I tell you to survey the Windows repair tools, and then bring up an Original Equipment Manufacturer (OEM) repair partition. Ha!

Anyway, your computer manufacturer might very well have a hidden partition on the system drive that contains an operating system image and all drivers for hardware that shipped with the system. This is a potentially valuable resource for you!

Start the computer and press F12; on most systems, this keystroke presents a list of all bootable media detected by the UEFI/BIOS. If you have a factory recovery partition, you can choose to boot from it, and you'll be prompted to reload your system.

Be advised that restoring your system drive via the factory recovery partition will in most cases reformat your system drive, which means you'll lose all data that you haven't already backed up.

### *Startup Repair*

Windows 8.1 and Windows 10 include a Startup Repair routine that's useful in cases where you suspect that some of Microsoft's own operating system files have become corrupted, replaced by incompatible versions by third-party software or malware, or have been inadvertently deleted.

Perform the “Shift Restart” technique I show you earlier in this chapter. (Open Start, hold down the Shift key, click the Power icon, and select Restart from the menu.) Next, from the Windows RE environment, select Troubleshoot ⇒ Advanced Options ⇒ Startup Repair. The computer automatically restarts, prompts you for a local administrator account password, and then performs the repair.

You may be prompted to insert your Windows installation DVD or USB drive if Startup Repair needs to replace one or more system files with “pristine” copies from the installation media.

## ***System Image Recovery***

System Image Recovery involves taking a snapshot of your entire system drive. This backup essentially clones your current Windows 8.1 or Windows 10 operating environment; therefore, you should create a System Image Recovery snapshot only when the system is in a healthy state.

To make a System Image Backup of your Windows 8.1 computer, follow these steps (the steps are the same for Windows 10):

1. **Click the Start button, then type File History, and press Enter.**

Unfortunately, the System Image Recovery tool is semi-hidden, and is part of the File History Control Panel.

2. **In the File History Control Panel, click System Image Backup in the lower-left corner.**

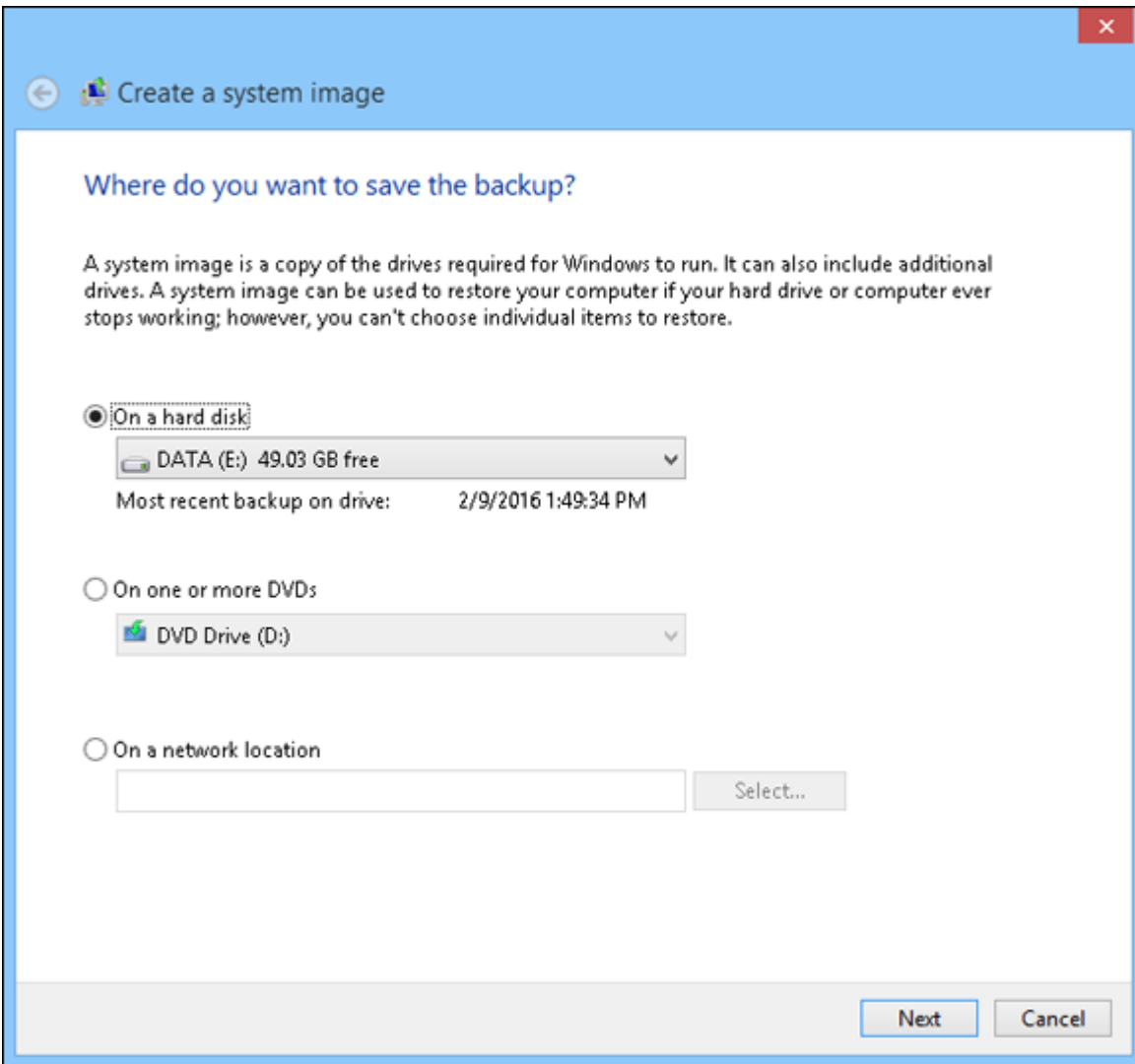
3. **In the Create a System Image dialog box (shown in [Figure 3-5](#)), choose a disk partition with enough room to host the image.**

You can't create a system image on your C: drive, because that's the partition that's being backed up. The system image will likely run into several gigabytes, so you may need to plug in an external USB drive of appropriate size.

4. **Click Next and select Start Backup to create your recovery image.**

Depending on how big your system drive is, the backup may take several minutes to several hours to complete.





**FIGURE 3-5:** Creating a system recovery image in Windows 8.1.

Restoring a previously created system recovery image is easy. Too easy, in fact.



**WARNING** Restoring a system recovery image replaces every last bit of content on your computer's system drive with the contents of the system image. Please make sure you're regularly backing up your user data.

To restore a system recovery image on a Windows 8.1 computer, follow these steps:

1. **Reboot the computer into Windows RE.**
2. **In Windows RE, select Troubleshoot ⇒ Advanced Options ⇒ System Image Recovery.**

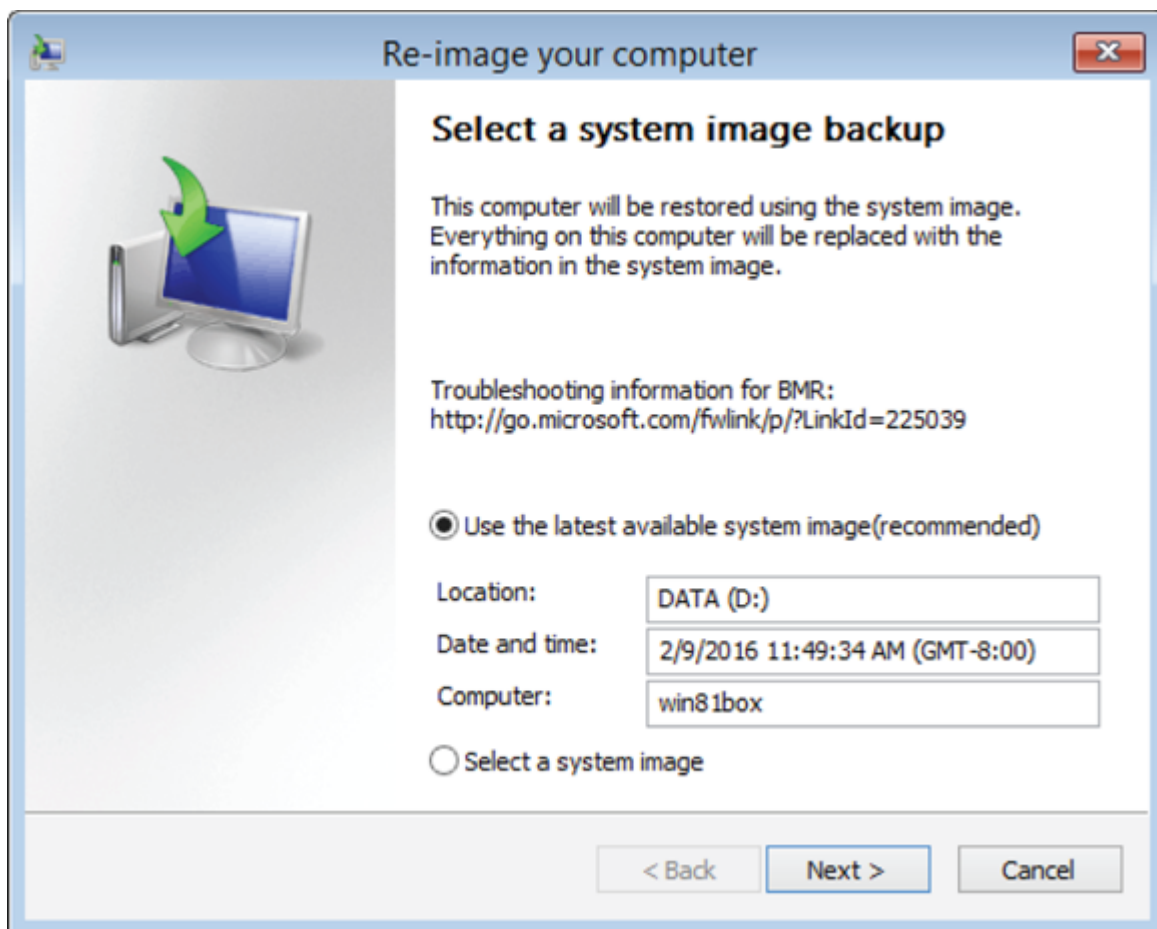
The computer reboots again, taking you directly into the System Image Recovery environment.

3. **In the Re-image Your Computer dialog box (shown in [Figure 3-6](#)), select the appropriate system image.**

By default, Windows shows you the most recent copy.

4. **Click Next, Next again, and then Finish to start the restore process.**

Think long and hard before clicking Finish, because the restore process will completely replace the contents of your system drive.



**FIGURE 3-6:** Restoring a System Recovery Image in Windows 8.1.

Although System Image Recovery can be a bit scary in its implications, I've used it to great effect in restoring customers' computers, especially those that have become hopelessly crippled with malware.

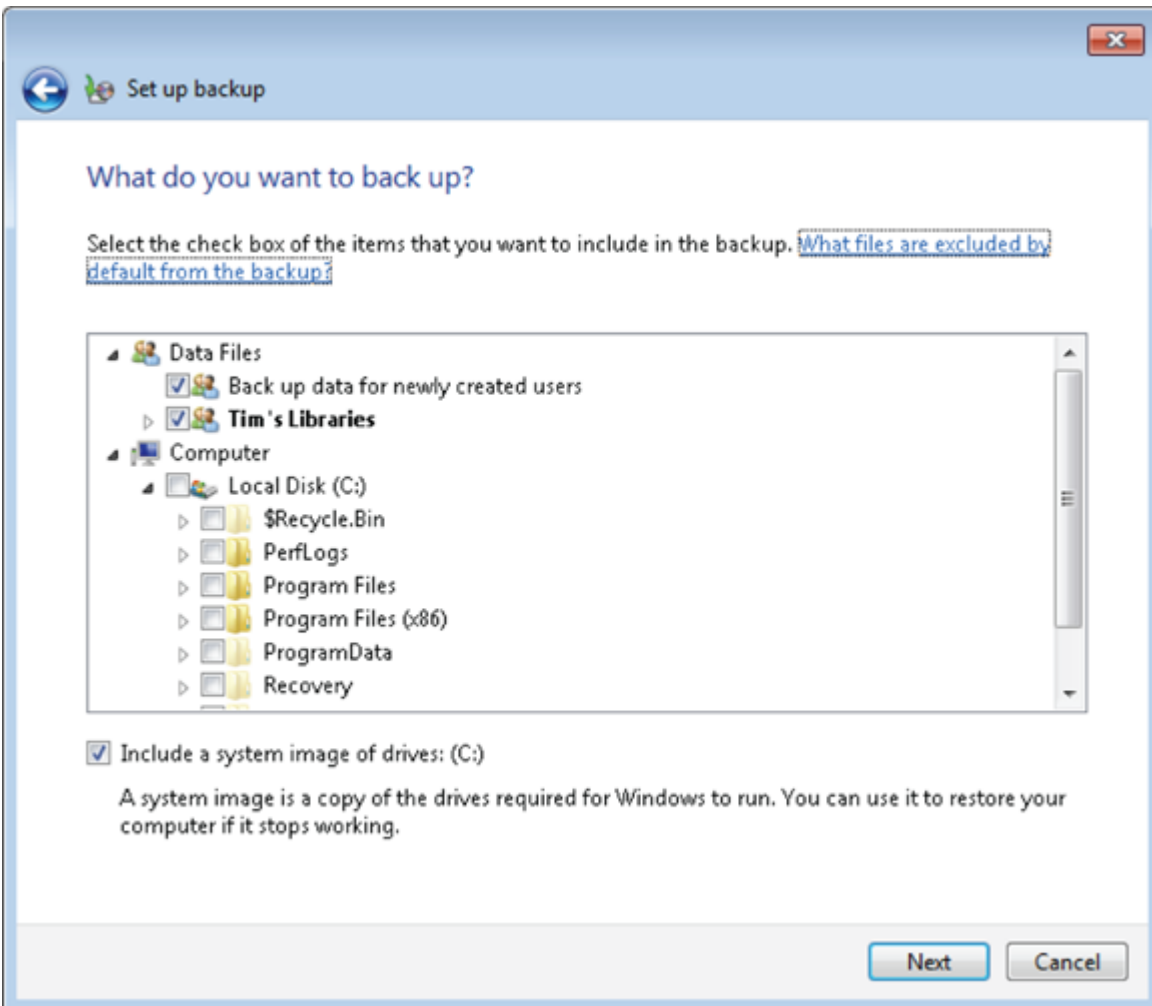
To make user data recovery as easy as possible, I encourage my customers to use public cloud file storage services like Microsoft's own OneDrive, or competitors like SugarSync or Dropbox.

## *Understanding Backup and Restore*

Ensuring data recoverability involves performing a *backup* (normally to another type of medium) in addition to storing the file on the hard drive. This medium could be (for example) another internal hard drive, a DVD-R, or an external USB disk.

If you have lost a single file (or all the files) on your hard drive, you will want to perform a restore. You need to have your backup files or tapes available and use the Windows backup utility to restore your files.

Windows 7 includes the traditional Windows Backup and Restore tool, which is available from the Start menu. Windows Backup uses a wizard interface, shown in [Figure 3-7](#), that allows you to pick and choose which files, folders, and data you want to back up.



**FIGURE 3-7:** The Windows 7 Backup and Restore tool is wizard-based and intuitive to use.



**FOR THE  
EXAM**

Know that the Windows Vista and Windows 7 backup tools allow you to create on-demand as well as scheduled backups.

### ***Critical applications and backup testing***

Before we continue, I need to double-underline two sometimes-overlooked but always relevant issues. First, please conduct a software inventory of your systems to ensure you're providing disaster recovery for critical applications.

Your business may be subject to service level agreements (SLAs), which define how long a critical application can remain offline before the company incurs penalties. Thus, I just wanted to remind you to include line-of-business applications in your backup and recovery planning.

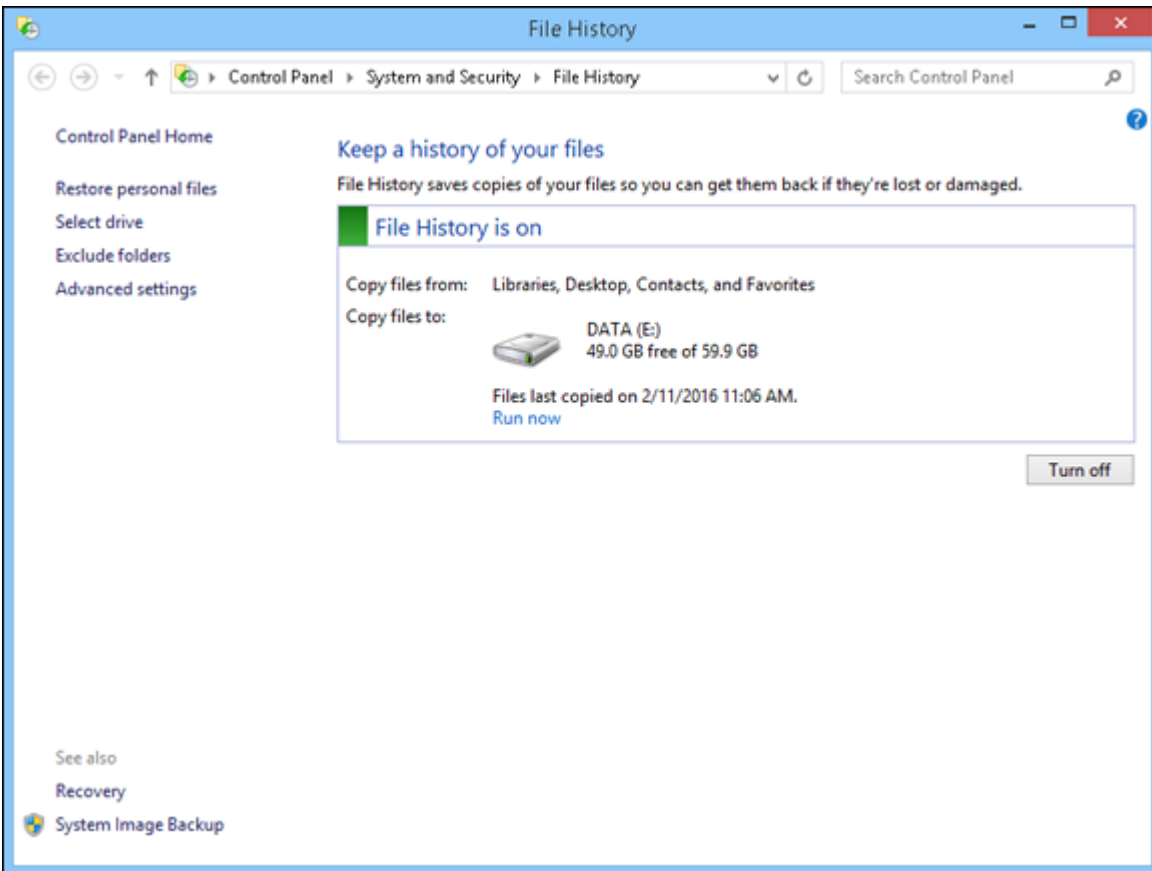
Along these same lines, you must remember that a good backup is only as good as its ability to be restored successfully. You need to ensure you're performing trial restores from time to time to verify that your backups are valid. Additionally, this practice helps you to remain calm during an actual emergency because you will have “been there, done that” numerous times already so you know what to expect from the process.

## *File History*

You need to pay particular attention to the Windows 8.1 backup and restore tools in order to be successful on the 1000-series A+ exams. To that point, Windows 8.1 and Windows 10 dramatically changed the backup and recovery landscape. You already learned about System Image Recovery; you also need to know about File History.

File History is very similar to the Time Machine feature in Apple macOS. Instead of the end user having to remember to create backups or schedule them, File History automatically backs up user data to an externally connected drive, another local hard drive, or to a network location.

To set up File History, open the File History Control Panel and click Turn On to start the service. This assumes that you have an appropriately sized data drive available to Windows. You can see in [Figure 3-8](#), for instance, that File History on my Windows 8.1 computer wants to use my E: data disk.

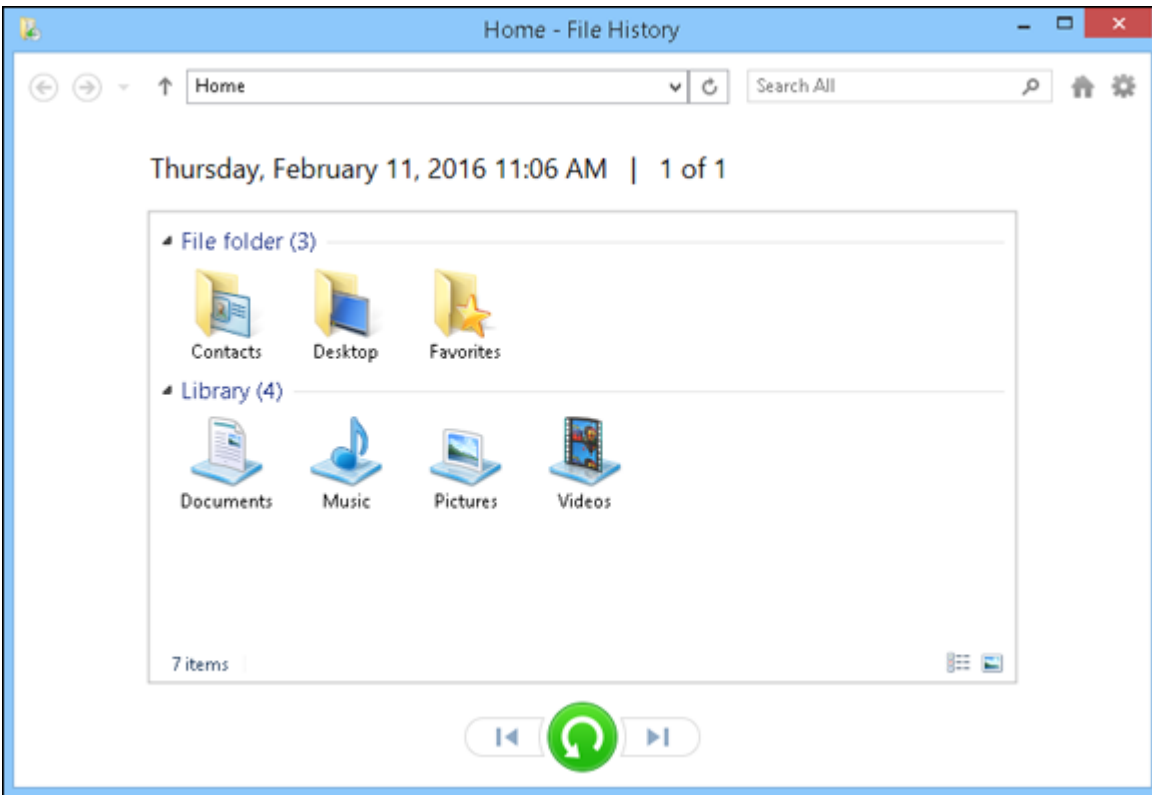


**FIGURE 3-8:** File History automates the backup of user data in Windows 8.1 and Windows 10.

Take a closer look at [Figure 3-8](#). Do you see the Select Drive option? That's where you go to choose which non-system disk you want to use for your File History backups.

Once you've enabled File History, Windows dutifully backs up your user data, including your document files, media files, Internet Explorer Favorites, and related irreplaceable assets. It's great!

Restoring deleted user data with File History is easy as well. Again, look at [Figure 3-8](#) and notice the Restore Personal Files link. That opens the recovery dialog box shown in [Figure 3-9](#). From here you can drill through the File History libraries to locate your missing assets, select them, and click the big green Restore button to put 'em back. Awesome.



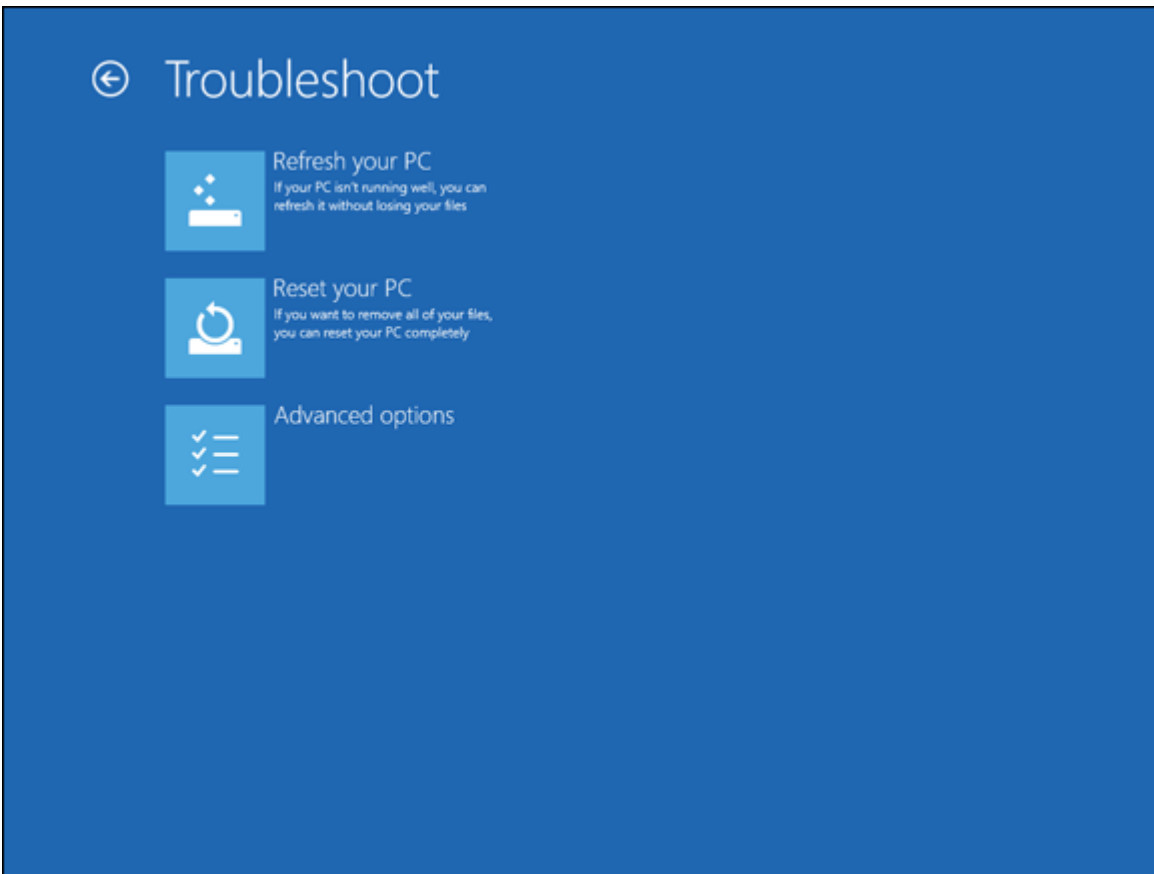
**FIGURE 3-9:** Restoring missing personal files by using File History is simple.

## *PC Refresh and Reset*

Windows 8.1 also gives you two nifty technologies that can assist you in two very different, but yet mission critical, scenarios. Let's say your Windows 8.1 system becomes super slow over time and otherwise “glitchy.” As one repair option among many that are available to you, you can restart the system into Windows RE and select Troubleshoot ⇒ Refresh your PC.

The PC Refresh process works similarly to the automatic system repair you look at earlier in this chapter, but with the exception that in a refresh, you're effectively re-installing Windows. Don't worry, though — all your user data remains intact.

By contrast, consider PC Reset (also accessible from the Windows RE Troubleshoot screen shown in [Figure 3-10](#)), which is useful when you're selling or giving away your computer and you need assurance that the local system drive is wiped completely clean.



**FIGURE 3-10:** PC Refresh and Reset are two valuable Windows 8.1 tools for any A+ repair technician.

In a Reset operation, the system drive is formatted, and Windows performs a “clean” operating system re-installation. It goes (almost) without saying that in this case, all user data is destroyed.

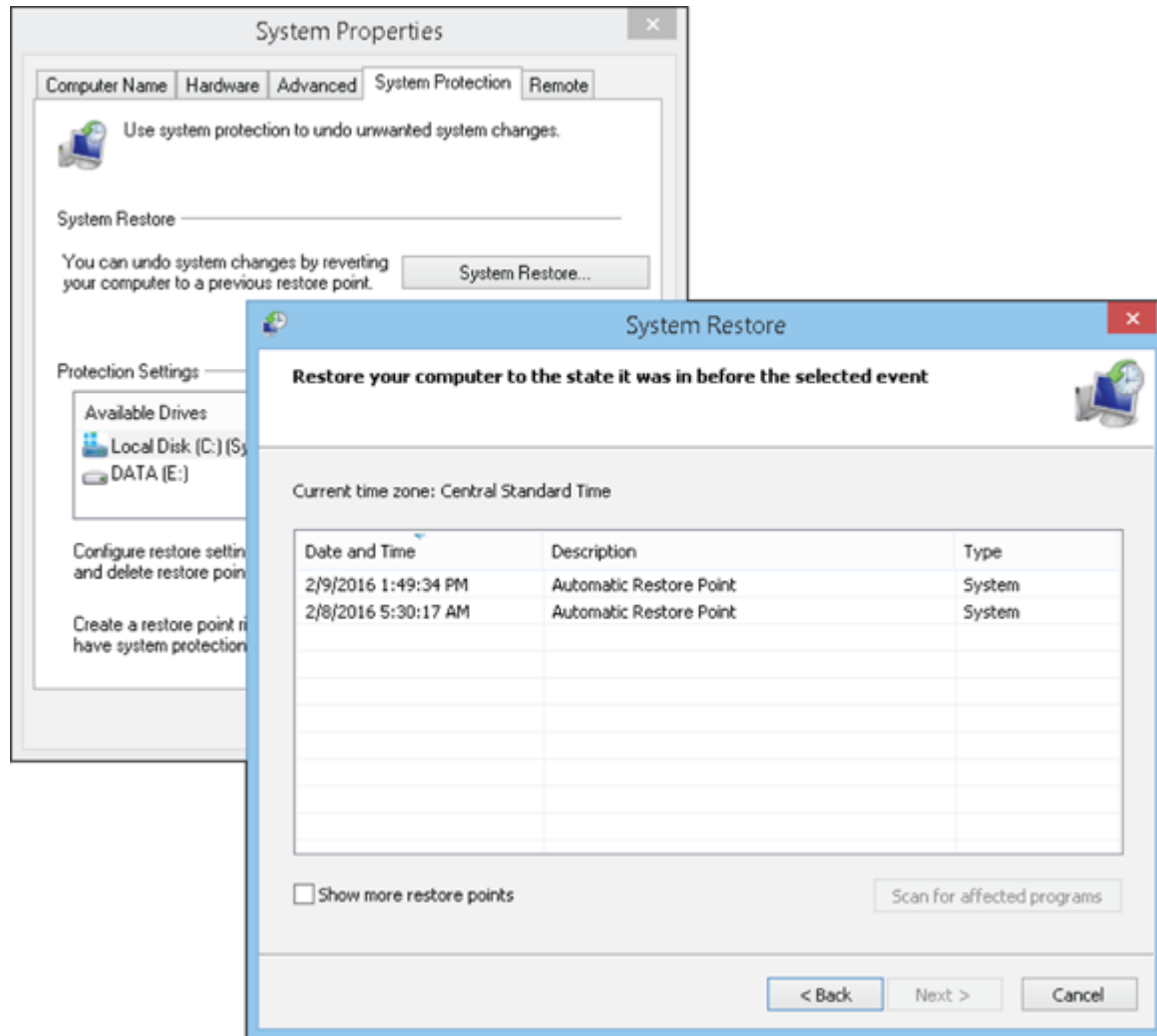
## *System Restore*

With Windows XP, Microsoft introduced a new system for backing out of driver changes — System Restore. When critical operations (say, updating drivers) are conducted on your system, Windows automatically creates a system restore point. This *restore point* can then be used to revert the system to a previous state in the event of an immediate failure. You can also manually create your own restore points.

If your computer encounters problems related to changes in its system files or settings, you can use a restore point (assuming that you have one saved) to quickly revert your computer to a previous state. It is like



having an Undo button for your OS, rather than needing to go through a full restore from backup. The System Restore Wizard interface is shown in [Figure 3-11](#).



**FIGURE 3-11:** The System Restore Wizard in Windows 8.1 and Windows 10.

### *Manually creating a restore point*

You can manually create a restore point from within the System Restore Wizard by following these steps:

1. **Choose Start ⇒ All Programs ⇒ Accessories ⇒ System Tools ⇒ System Restore.**

In the System Restore dialog box that opens (refer to [Figure 3-11](#)), you can

- Restore My Computer to an Earlier Time
- Create a Restore Point

**2. Select Create a Restore Point and then click Next.**

**3. Provide a description and click Create.**



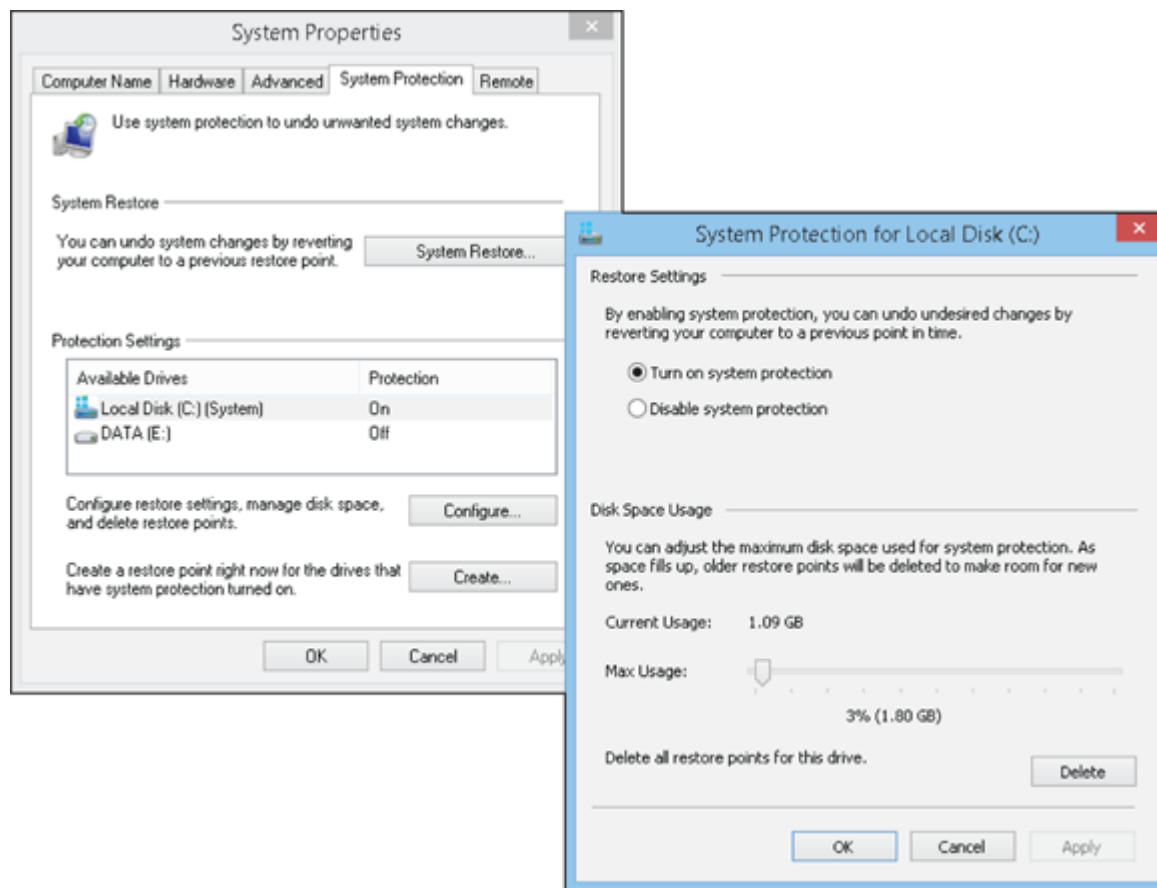
**TIP**

A restore point description makes it easier to locate an appropriate restore point during the restore process.

**4. When the creation process is complete, click Close to exit System Restore.**

For Windows Vista and Windows 7, you create a restore point by opening the System Protection tab of the System Control Panel and clicking the Create button, which will ask you for a description of the restore point.

For the System Restore to work, Windows monitors all hard drives on your system. Windows Vista defaults to letting you use up to 12 percent of your drive space for System Restore data, while Windows 7 and later are a little more dynamic in assigning an initial percentage, maxing out at 100 percent. This system restore cache setting can be adjusted by choosing Start ⇒ Control Panel and double-clicking the System applet. Then click the System Restore tab. [Figure 3-12](#) shows the dialog box and the settings for the c: drive, which I accessed by selecting the drive and clicking the Settings button. You can adjust the system restore cache by moving the slider and clicking OK.



**FIGURE 3-12:** Changing the System Restore cache size.

Reducing the size of the cache reduces the disk space used by System Restore but also reduces the number of restore points that Windows will keep track of for you, which also reduces the age of your oldest restore.

If you have only one partition or drive on your computer, you can adjust the cache size without going into the settings for the disk.

### ***Restoring your computer to a previous state***

Minor and major disasters can require you to access a restore point to return your computer to working condition. The following instructions guide you through restoring your computer to a previous state by accessing a system restore point:

1. **Choose Start ⇒ All Programs ⇒ Accessories ⇒ System Tools ⇒ System Restore.**

The System Restore Wizard (refer to [Figure 3-4](#)) gives you the following option:

- Restore My Computer to an Earlier Time
2. **Select Restore My Computer to an Earlier Time and then click Next.**

The wizard presents you with a list of restore points.

3. **Select the appropriate restore point and then click Next.**

You see a warning you that you will lose recent changes on your system if you choose to restore.

4. **Click Next or Finish.**

Your system reverts to how it was configured at the restore point you chose, and your computer reboots.



ON THE  
WEB

Labs 3-1 and 3-2 provide practice creating and invoking a system restore point in Windows 8.1 and Windows 10. The labs can be downloaded from the companion website at

[www.dummies.com/go/aplusaio](http://www.dummies.com/go/aplusaio).

## *Recovery and Rescue Methods*

So far in this chapter, you have seen many different tools that you can use to repair your computer when it is in a non-booting state. This section looks at manufacturer recovery tools, third-party tools, and special Windows installations.

### *Recovery DVDs, USB drives, and recovery partitions*

Many large computer companies, such as HP and IBM, provide a quick way to restore your computer to its default factory installation. In the past, this was done by using recovery CDs. When you unboxed your computer,

you would get a set of bootable CDs that held some type of image of your computer. If your computer became unusable because of a virus, hard drive failure, or other issue, you could quickly boot from the CDs and restore your computer to its factory state. One problem with this scenario is that it usually meant that you also lost all your data if it was not otherwise backed up.

Over the years, with vendors prepackaging applications with their computers, the size of that factory image has gotten larger and larger, so that now it would take multiple CDs, or even multiple DVDs, to store all that data. This change in the preparation of the computers has caused some vendors to use a recovery partition instead. This hidden partition contains the tools needed to restore the image to the rest of the hard drive. If you use partitioning tools and delete the partition, you lose your ability to restore the system to its factory default settings. The vendor will usually, however, give you the ability to back up this partition to CDs or DVDs. Usually, this partition is accessed by pressing one of the computer's function keys during boot-up.

Microsoft offers a free Media Creation Tool that makes it simple to populate a blank USB flash drive (also called a "thumb drive") with the Windows 10 installation media. For instance, I myself haven't needed to use a physical DVD in many, many years thanks to ISO software files and USB sticks.

## ***Recovery image***

In addition to factory images that are available from some hardware vendors, you have the option of making your own recovery image. You can store this image on a partition on your hard drive, on a network server, or on some type of removable media. To create and restore this image, you can use some type of imaging software, such as O&O Software's DiskImage. These tools allow you to create your own custom image to be used for recovery purposes.

## ***Rescue CDs***

A *rescue CD* is a bootable CD that includes tools used to rescue files from a failing hard drive, or to repair problems that occurred with a

Windows installation that made it non-bootable. Many third-party rescue CDs are available to the CompTIA A+ Certified Professional. Some rescue CDs are commercially available, but a wide variety of them are available for free. A quick Internet search for *Live CD* will reveal a wide range of these CDs. It seems that there are as many types of custom Live CDs as there are problems that you need to solve. With a little searching and experimenting, you can find one that meets your most common problems to add to your arsenal of tools.



TECHNICAL  
STUFF

Many of the key rescue CDs I have used for years are now actually DVDs. (With the extra space for tools, these DVDs are more useful than ever.) You can take the term “rescue CD” to mean “CD or DVD” in this section.

You’ll find discussion of any rescue optical media more in the Linux world, if my experience is any indication. Practically speaking, though, in the twenty-first century, computer repair technicians are far more likely to use USB thumb drives as repair platforms.

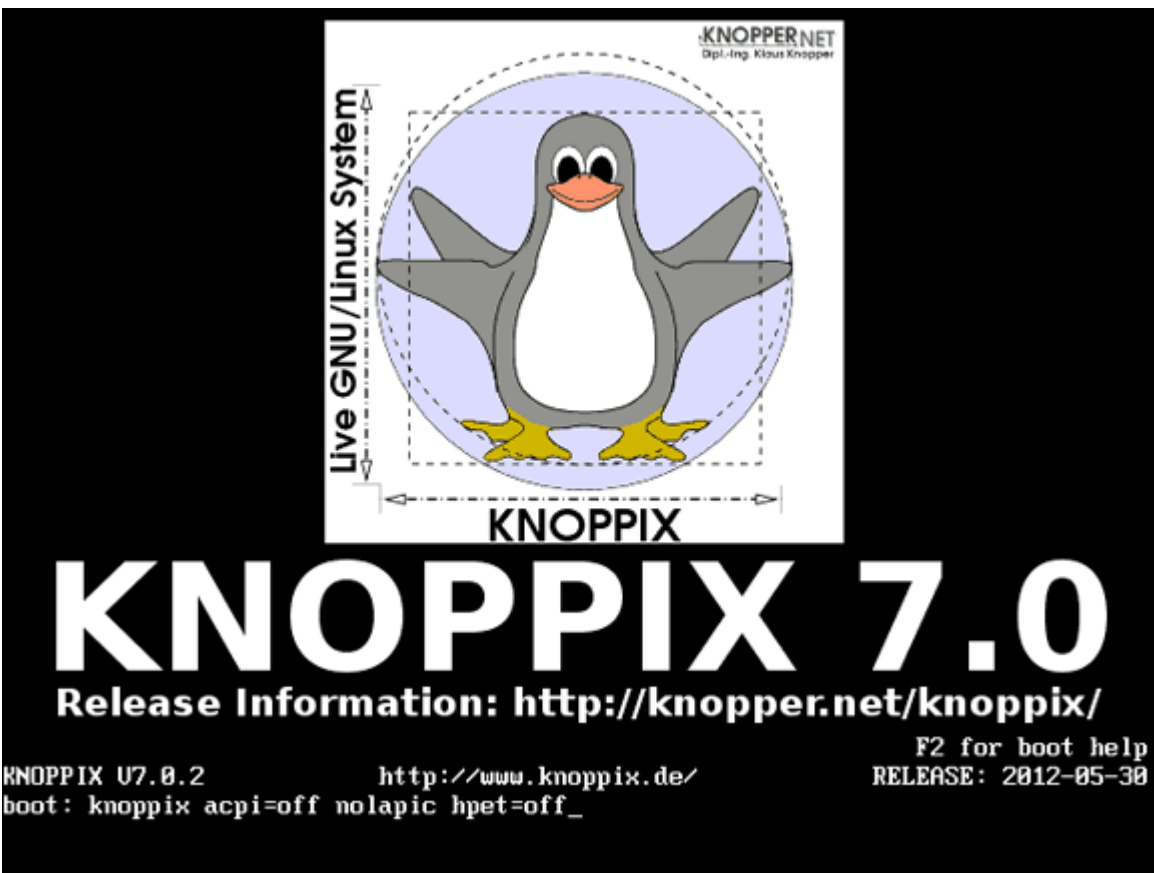
Many rescue CDs run a version of Linux, which has been prepackaged onto a bootable CD or CD image that includes a variety of tools. Knoppix, running a version of Debian Linux, is just one of these Live Linux CDs that many people use as a rescue CD, partly because it has a wide selection of tools and partly because it includes a GUI in the form of the X Window System and KDE or GNOME. With the variety of applications bundled on the Knoppix CD and the fact that the system runs entirely off of the CD, Knoppix is a great way to try Linux without having to install it. The following offers a brief overview of some of the rescue options that are available to you when using Knoppix, and most of the other Live CDs offer a similar mix of features. Try a few to find one that works for you.



**TIP**

Conveniently enough, Wiley also publishes *Linux Bible*, Ninth Edition, by Christopher Negus. It covers Knoppix as well as many of the tools you will need to know how to use to diagnose and resolve problems with your Linux installation. With this book, you will be able to do a Linux deep dive; the book will guide you through Linux management from start to finish, including a Linux installation on a flash drive, which can be used in place of a rescue CD.

The Knoppix boot process starts off with a confirmation of your intention to boot into Knoppix, as shown in [Figure 3-13](#). There are advanced boot options that you can access or get information about by pressing F2 or F3, but in most cases, the system will boot without additional information.

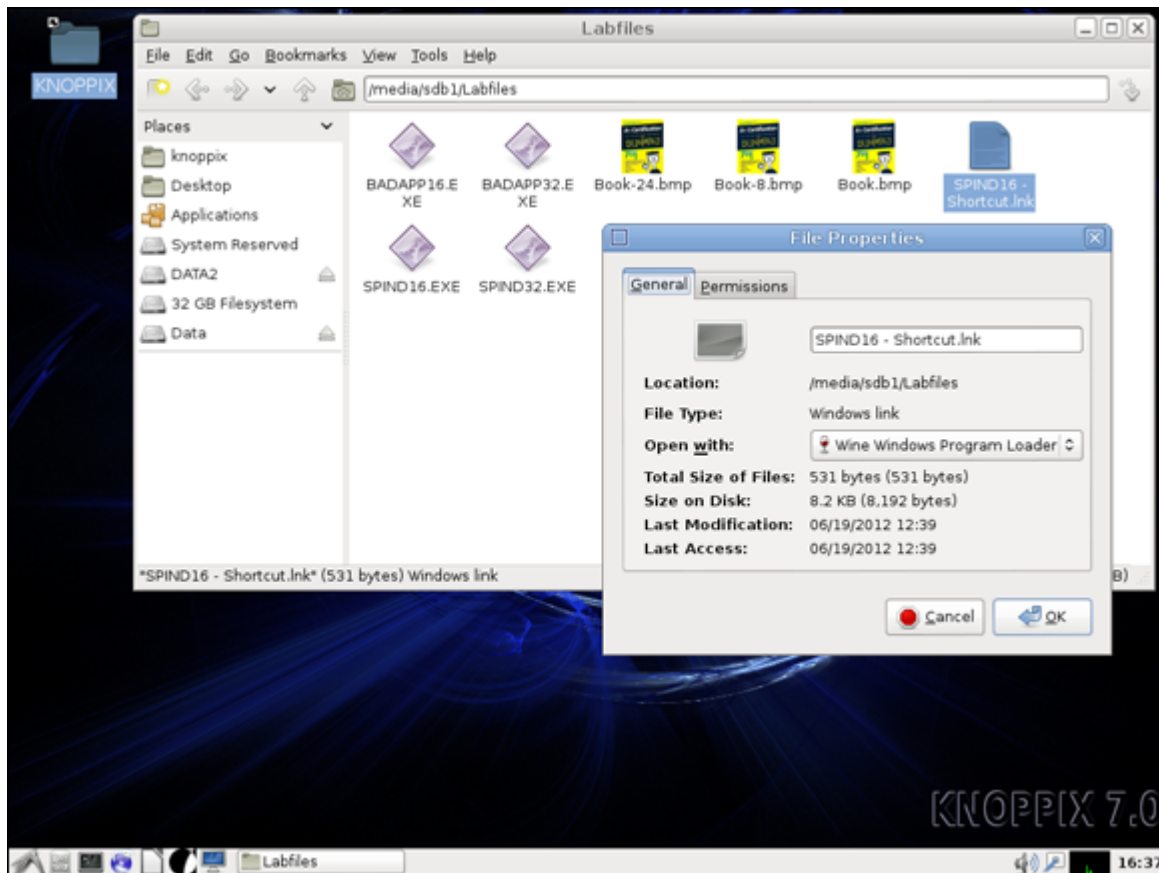


**FIGURE 3-13:** If your computer has unique hardware, you might need to use special boot options.



**TIP**

If you are not familiar with Linux, here's a pointer: Linux identifies hard drives with letters and partitions with numbers, so in a typical IDE/ATA system, your four devices or drives are identified as `hda`, `hdb`, `hdc`, and `hdd`, with the `C:` drive usually being `hda1` (the 1 means partition 1); while on SATA or SAS systems your first four devices or drives are identified as `sda`, `sdb`, `sdc`, and `sdd`. In the case of Knoppix, all local disk partitions are automatically mounted for access and will appear on the desktop; some versions may only mount them as read-only. You can change the properties of the disk to allow writing to it; otherwise, you can browse and read files on your system. [Figure 3-14](#) shows the properties of a Windows shortcut file that is found on `sdb1` in a `labfiles` directory.



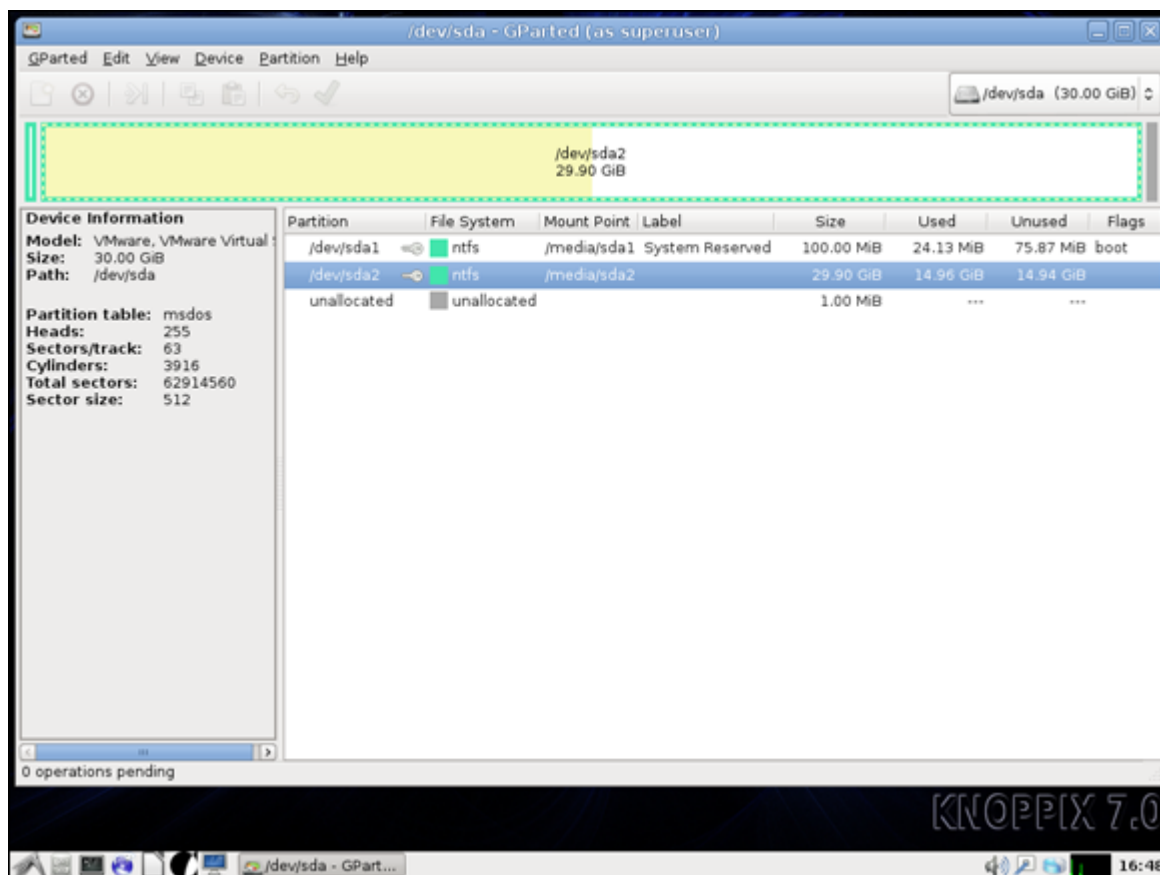
**FIGURE 3-14:** Local files can be managed and many settings viewed.



The overall desktop should not be alien to Windows users, with an applications menu in the bottom left of the screen, where the applications are stored in categories like Accessories, Education, Games, Graphics, Internet, Office, Sound & Video, and System Tools. Version 7 of Knoppix also includes WINE (a Windows environment for running Windows programs) which may be able to run some of the applications on your hard drive.

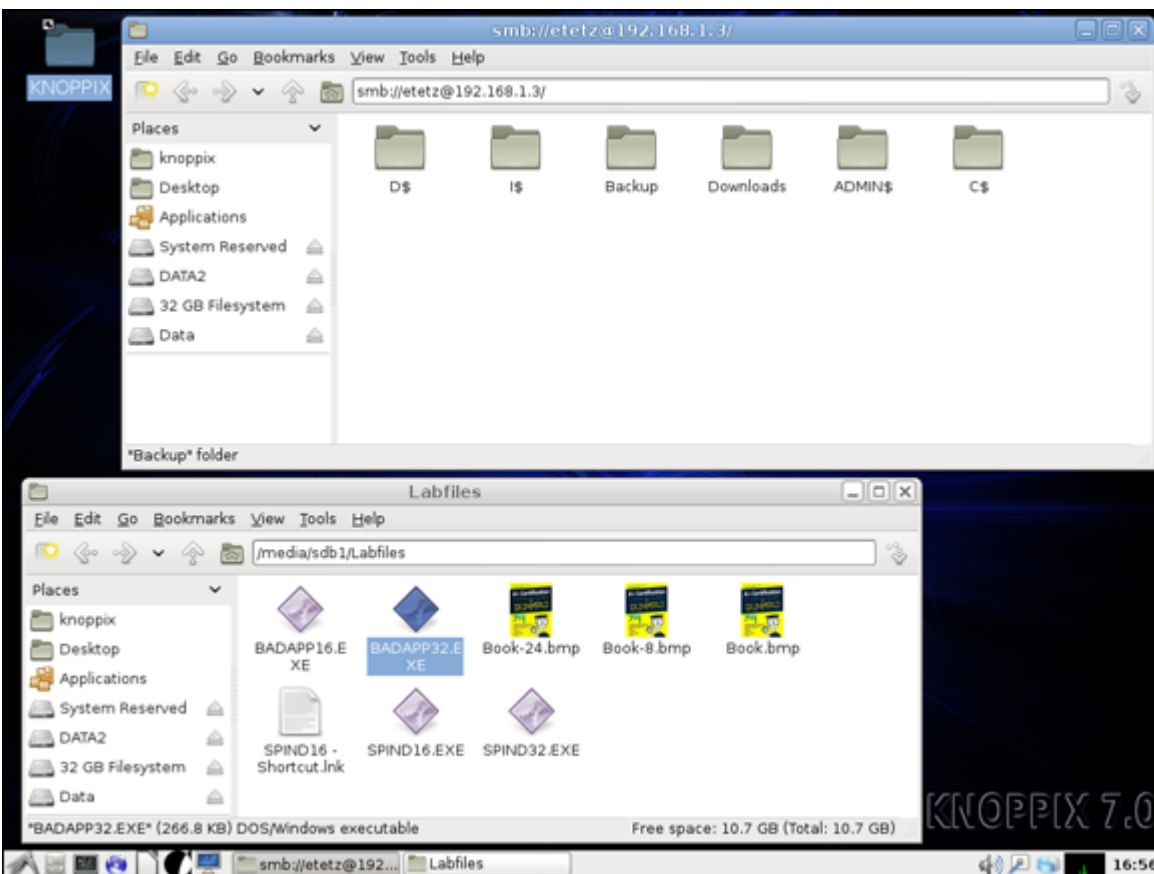
With the tools on this Live CD, you can verify many settings and even modify files that are found on your Windows installation.

Knoppix has several tools that you will likely find useful, such as `partimage` (partition image; allows you to perform disk imaging tasks on your partitions) and `parted` (a command line, disk partition–editing tool). [Figure 3-15](#) shows the interface of GParted (a GUI front end for `parted`). This interface is reminiscent of Partition Magic. You can use GParted to create, resize, delete, and move partitions around your drive.



**FIGURE 3-15:** The disk partition management is easy to use after you understand how Linux refers to disks and partitions.

To copy files to or from a Windows server on your network, you can use tools like Samba Network Neighborhood to access shared folders on your servers. You can use this tool to copy network drives to a computer that doesn't have them or to rescue files from a hard drive that is very near failure and can no longer support booting. [Figure 3-16](#) shows the shares that are available on the server 192.168.1.3 as well as in a folder on the local hard drive, making it easy to move data between locations.



**FIGURE 3-16:** Files may be transferred to and from file servers.

## *Rescue partitions or rescue installations*

Many of the quickest ways to repair a Windows installation are actually built into Windows. To repair a Windows installation from a Windows installation, you need only a small amount of planning. If you leave some free, unpartitioned space on your hard drive, you can create a rescue

partition. A *rescue partition*, or *rescue installation*, of Windows is simply another copy of Windows that is installed onto your computer.

This second copy of Windows is not the default for booting, and is used only to repair problems to your normal installation of Windows. So if your default copy of Windows is installed on drive C :, your rescue install could be installed on drive D : or drive E :. The partition should be used only for the Windows installation, and not used to store data for your normal installation. After installing Windows in the second location, it will be automatically set as the default boot. To change the default booting installation of Windows, follow these steps:

1. **Choose Start ⇒ Control Panel.**
2. **If your Control Panel folder displays in Category view, choose Performance and Maintenance ⇒ System; if your Control Panel folder displays in Classic view, double-click System.**
3. **In the System Properties dialog box that opens, click the Advanced tab and then on Settings in the Startup and Recovery section.**
4. **In the Startup and Recovery dialog that opens, choose the copy of Windows that you would like to be the default booting installation from the Default Operating System drop-down menu.**
5. **Click OK twice to close both open dialog boxes.**



**TIP** I'm sure you've noticed by now that in Windows 10, you have both the classic Control Panel programs as well as the new, flashy Settings pane. Although the Windows developers plan to move most or all Windows configuration options to the Settings pane, they aren't there yet. Thus, you need to accept the fact that you'll be using both interfaces for the foreseeable future.

## *Scheduling Preventive Maintenance*

This chapter walks you through the process of creating scheduled backups to keep your data safe. In addition to backups, many maintenance tasks can be scheduled to keep your computer running smoothly and safely. At a minimum, thought should be given to scheduling at least the following tasks:

- » **Disk defragmentation:** This task will optimize the files on the drive to improve disk access speeds. To read more about this tool, review Book 2, [Chapter 5](#).
- » **Check disk utility (chkdsk.exe):** This task will examine the disk files and directory structures for errors. If errors are found, you can rerun the tool to fix errors. To find out more about this tool, look at Book 2, [Chapter 5](#).

To schedule a task, choose Start ⇒ All Programs ⇒ Accessories ⇒ System Tools ⇒ Task Scheduler. Disk defragmentation should have a default system task, so navigate in the left pane to Task Scheduler Library ⇒ Microsoft ⇒ Windows ⇒ Defrag. Ensure that the task `ScheduledDefrag` has a status of Ready; otherwise, right-click the task and choose Enable.

`chkdsk.exe` does not have a default system task, so to review how to create a schedule for a task, look into Book 6, [Chapter 4](#). When creating the task, set the command to execute to `cmd /k %systemroot%\system32\chkdsk.exe C:.` When this task runs, it will cause a command window to open, which will remain open until you close it.

Of course, the scheduled tasks I've given you thus far barely scratch the tip of the proverbial iceberg. Keep the following in mind as well:

- » **Windows Update:** Microsoft releases Windows-related security fixes and performance improvements on the second Tuesday of every month (what many systems administrators call “Patch Tuesday”).
- » **Anti-malware definitions:** Unless your system is equipped with the latest and greatest anti-malware signatures, it will be unable to defend against any “nasties” that make their way to your computer.

- » **Driver/firmware updates:** What's cool about Windows Update nowadays is that it can update third-party software in addition to native Windows code. This means that you largely don't need to worry about keeping your hardware drivers current anymore.

Although I focus on Windows almost exclusively in this chapter, all the best practices I outline apply equally to macOS and Linux.

## *Getting an A+*

This chapter helps you prepare for disasters by covering the following topics:

- » Using the various Windows backup and recovery utilities to protect your data
- » F8 boot options that can be used to correct startup problems on older Windows systems
- » System restore points and how to use them to repair configuration problems
- » Recovery and rescue CDs, DVDs, USB drives, and partitions

## *Prep Test*

- 1. Which of the following keys should you press in the Windows 10 Start menu in order to restart the system into Windows RE?**
  - (A) Del
  - (B) Alt
  - (C) Ctrl
  - (D) Shift
- 2. Windows 10 includes the Windows Backup and Restore utility.**
  - (A) True
  - (B) False

**3. A user bought a new video card with 4GB of RAM. He needs it to play the new version of his favorite video game. After installing the video card, he boots up his Windows 8.1 computer and is overjoyed when he sees the Plug and Play Wizard detect the new hardware. When prompted, he provides the driver disk that came with his computer. After loading the driver for his new video card, his computer reboots. During the next boot, his computer halts and will not respond to any controls. What should he do next?**

- (A) Reboot his computer by using the power button. His computer will automatically boot to the Last Known Good Configuration.
- (B) Reboot his computer by pressing Ctrl+Alt+Del and then pressing when he sees the message to Press F8. He will then be able to choose Disable Advanced Video Options from the boot menu.
- (C) Reboot his computer by using the power button. His computer will automatically display the boot menu and attempt to boot to Last Known Good Configuration without user intervention.
- (D) Reboot his computer by pressing Ctrl+Alt+Del and then hold down F9 to enable Safe Mode.
- (E) Reboot his computer by using the power button. When he sees the message to Press F8, press it and select either the Last Known Good Configuration or Enable VGA Mode.

**4. Which of the following actions should you perform when you prepare a Windows 8.1 computer for resale?**

- (A) You should run a PC Reset.
- (B) You should run a PC Refresh.
- (C) You should disable File History.
- (D) You should boot into Safe Mode.

**5. You can store a System Recovery Image on your Windows 10 computer's C: drive.**

- (A) True
- (B) False

**6. System Restore does not affect user data.**

(A) True

(B) False

## *Answers*

1. **D.** The easiest way to get into Windows RE from Windows 10 is to navigate to the Start Screen, hold down the Shift key, open the Power menu, and select Restart. *See “Accessing startup settings in Windows 8.1 and Windows 10.”*
2. **B.** This is false. Instead, Windows 10 gives you File History, System Image Recovery, and PC Reset/Refresh. *Peruse “Accessing startup settings in Windows 8.1 and Windows 10.”*
3. **E.** Either of these two options, Last Known Good Configuration or Enable VGA Mode, will allow him to boot his computer. If he chooses to boot the Last Known Good Configuration, any changes that he made to the hardware configuration since the last boot will be lost. If he chooses the Enable VGA Mode, he will be able to select a different driver to be used by the graphics controller or apply other software patches to get the system running. Safe Mode should be his next step on correcting the problem. *Peruse “[Using F8 Options during Boot-Up.](#)”*
4. **A.** In Windows 8.1, the PC Reset option is great for when you need to remove all personal information from a Windows 8.1 computer. *See “Accessing startup settings in Windows 8.1 and Windows 10.”*
5. **B.** This is false. Because the System Recovery Image process creates an image of your system (C:) drive, you need to store the image elsewhere. *Peruse “[System Image Recovery.](#)”*
6. **A.** This is true. System Restore affects only the operating system and application files, not user data. *Make note of “[System Restore.](#)”*

# **Book 8**

# **Networking**

## **Contents at a Glance**

### **Chapter 1: Down to the Networking Basics**

[Identifying the Types of Networks](#)  
[Understanding Network Topologies](#)  
[Connecting with Network Cabling](#)  
[Troubleshooting Networking Cables](#)  
[Examining Network Access Methods](#)  
[Piecing Together the Network Architectures](#)  
[Understanding Network Protocols](#)  
[Working with Network Devices](#)  
[Understanding Communication Methods](#)  
[Ways to Network a Computer](#)  
[Troubleshooting Networking Issues](#)  
[Getting an A+](#)  
[Prep Test](#)  
[Answers](#)

### **Chapter 2: Understanding Common Wireless Communications**

[Understanding Infrared Devices](#)  
[Working with Wireless Networks](#)  
[Installing and Configuring a SOHO Network](#)  
[Other Wireless Connections](#)  
[Increasing Wireless Network Performance](#)  
[Troubleshooting Issues](#)  
[Getting an A+](#)  
[Prep Test](#)



[Answers](#)

## **Chapter 3: Networking the Operating System**

[Understanding Networking Components](#)

[The TCP/IP Protocol](#)

[VLANs](#)

[Understanding Name Resolution](#)

[Looking at Protocols and Ports](#)

[Troubleshooting with TCP/IP Utilities](#)

[Sharing File System Resources](#)

[Sharing Printer Resources](#)

[Networking with Windows](#)

[Understanding Windows Services](#)

[Getting an A+](#)

[Prep Test](#)

[Answers](#)

## **Chapter 4: Configuring Internet Access and SOHO Networks**

[Understanding the Internet](#)

[Using an ISP](#)

[Working with an ASP](#)

[Understanding Internet Protocols](#)

[Installing and Configuring Browsers](#)

[Using the Internet](#)

[Ways to Access the Internet](#)

[Installing a Small Office/Home Office \(SOHO\) Network](#)

[Firewalls and Home Routers](#)

[Getting an A+](#)

[Prep Test](#)

[Answers](#)

# Chapter 1

## Down to the Networking Basics

---

### IN THIS CHAPTER

- » Identifying network types
  - » Understanding network topologies
  - » Working with network cables
  - » Becoming familiar with network architectures
  - » Accessing the network
  - » Installing a Small Office/Home Office (SOHO) Network
- 

The A+ certification exams cover two areas of networking: networking theory/networking hardware and networking at the operating system (OS) level. This chapter focuses on the networking theory and the networking hardware area of the A+ exams. For the exams, you are required to know popular terms and features of networking environments that you will encounter on the exams and in the real world — which is what this chapter will help you with. Networking at the OS level is covered in [Chapter 3](#) of this minibook.

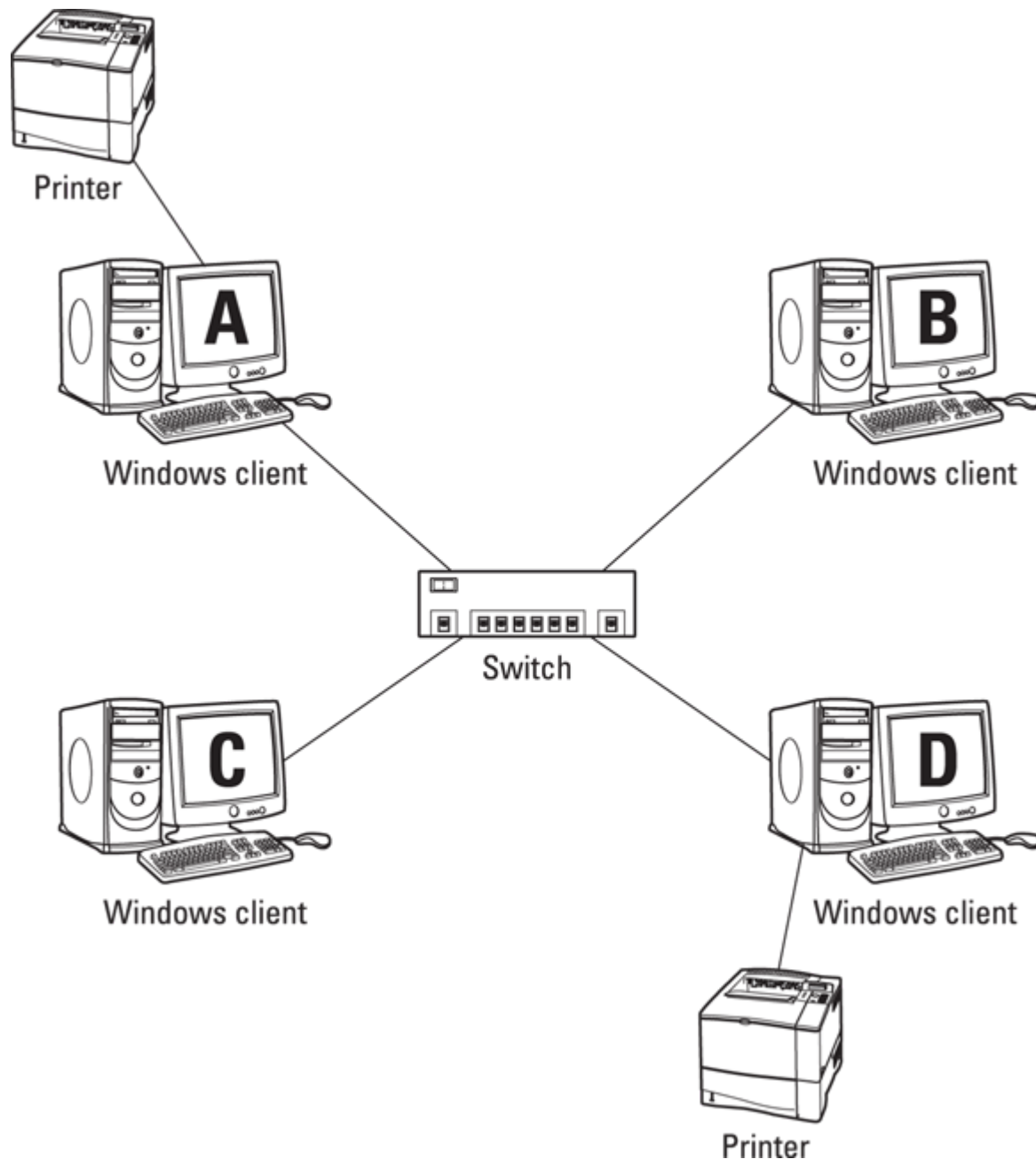
## *Identifying the Types of Networks*

A *network* is a group of connected systems for sharing data or devices. This section provides an overview of the two major types of networks: peer-to-peer and server-based (client-server). I discuss the advantages and disadvantages of each type as well as how to implement them.

### *Peer-to-peer networks*

In a *peer-to-peer* (P2P) network, all systems connected to the network can act as clients or servers. A *client* is a system that makes a request for a resource or service on the network; a *server* is the system providing the

resource or service. In this type of networking environment, all systems are considered equal because they can all play the same roles on the network — either as client or server or as both client and server. The recommended number of systems in a P2P network usually involves ten or fewer systems because of the lack of centralized administration. As a network administrator working in a P2P environment, you will constantly run from machine to machine to perform administrative tasks. Typically, a P2P network involves each system running a desktop operating system, such as Windows 8.1 to provide network functionality (see [Figure 1-1](#)).



**FIGURE 1-1:** Peer-to-peer network environments.

In [Figure 1-1](#), notice that client A provides a network resource — a printer — as does client D. This shows that client A is acting as both a server and a client, which is the purpose of a P2P network.

Because a central machine doesn't store files in a P2P network, your networking environment isn't based on the centralized administration approach. With *centralized administration*, you (as network

administrator) could perform network administration tasks for the entire network from one place. Looking back to [Figure 1-1](#), you can see that because all four computers act as *peer servers* (meaning they all act as servers to one another), you need to do the administration on all four computers — a major disadvantage of P2P networking.

Some examples of the administration you must perform on each system are creating user accounts on each computer and managing file and folder sharing from each system. In [Figure 1-1](#), for example, if you want Bob to log on to client A, you would create the Bob account on client A. At the same time, if you want Sue to log on to client B, you would create the Sue account on client B. Because the Bob account doesn't exist on client B, Bob can't log on to that computer even though he might be able to access the files on client B from client A. This leads to a *distributed administration* model because your work is spread across multiple machines.

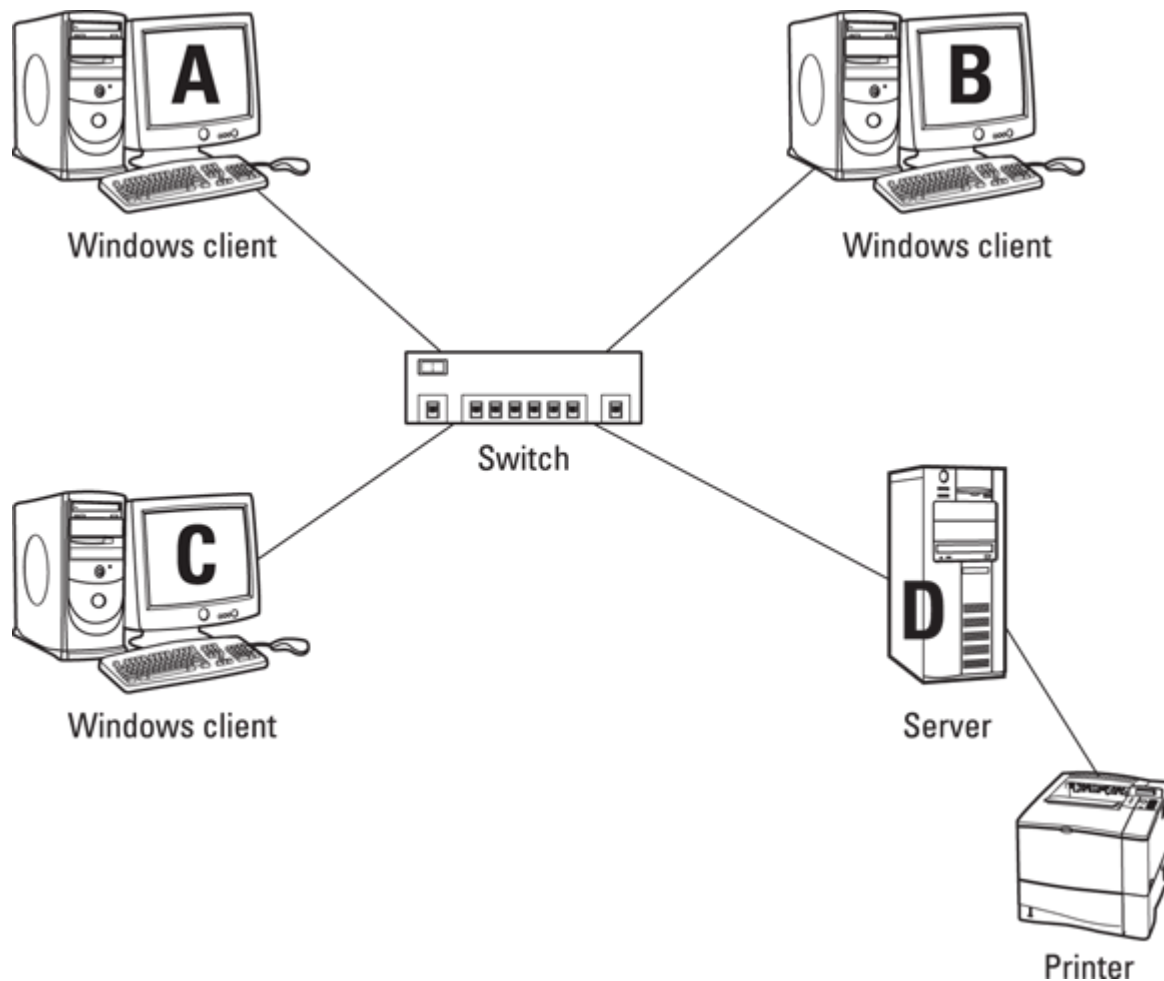
The major advantage of P2P networking is that you save money by not needing to purchase a central server, which can cost thousands of dollars in hardware and software. Too, with a P2P network, you also don't have to purchase a separate network operating system (NOS). A NOS, required on a server-based network (discussed in the next section), is designed for networking services (such as Dynamic Host Configuration Protocol [DHCP], web, file, and print services) and allows the server to share its files and printers with clients on the network. The cost of the NOS, and the licenses to have clients connect to the server, is where a number of large companies spend most of their IT budget. Licensing is expensive!

## ***Server-based (client-server) networks***

*Server-based* networking, also known as *client-server* networking, is the networking model that most companies usually choose for ten or more workstations on a network. Unlike a P2P network, server-based networking uses a central machine (the server) that delivers network services to the workstations. Once again, these network services could be services such as file and printer sharing, user account authentication, or web services.

The benefit of a client-server configuration is that you can leverage centralized administration by performing the bulk of your work on the one server. For example, if you need to create user accounts for each of the ten users, you create the ten accounts on the one server. Compare that with a P2P network, where one account is created on each system. As the administrator of this network, you create all shared directories on the server along with user accounts so that the server may verify the credentials of a client who attempts to log on to the network. All users on the network connect to this server to save and retrieve files.

Tighter security is another benefit of using a server-based networking model. Creating a more secure environment is easier with a server-based network because your resources and user accounts are not spread across multiple machines. Looking at [Figure 1-2](#), you can focus on the server because it contains the files, folders, and user accounts. When a user logs on to the network, the logon request is sent to the server, which verifies that the username and password are valid. After a user is logged on, the server allows the user access to resources, such as files and printers, that the user has permission to use. [Figure 1-2](#) illustrates a server-based networking environment.



**FIGURE 1-2:** Server-based networking environment.

Notice in [Figure 1-2](#) that the client systems connect to the server to access the printer. In this environment, all systems have a defined role: They are either a client or a server — but not both.

The disadvantage of using a server-based environment is the cost of purchasing the server hardware and the NOS. When designing your networking model, make sure that you work with someone familiar with software licensing so you get the best bang for your buck!

### ***Server roles***

When creating a network, you can install servers that provide a number of different types of functionality to the network. Following is a list of the common types of server roles that exist on networks today:

- » **Web server:** A web server delivers web pages to clients using the HTTP or HTTPS protocol. Web servers host public websites or intranet sites used inside a company.
- » **File server:** A file server stores data documents such as Microsoft Word, Excel, and PowerPoint files. The file server typically offers permission capabilities so that you can control who can access what files.
- » **Print server:** A print server is used to share printers with network clients and queue print jobs while they are waiting to be printed.
- » **DHCP server:** A DHCP server is responsible for handing out IP addresses to clients on the network so that you do not need to run around to each client and manually configure an IP address.
- » **DNS server:** A DNS server is responsible for translating fully qualified domain names such as [www.glenecclarke.com](http://www.glenecclarke.com) to its IP address.
- » **Proxy server:** A proxy server is responsible for sending requests to the Internet on behalf of the user. A proxy server adds a layer of security, in that the user is not sending the request to the Internet directly. A proxy server typically has NAT features and policy features to control which websites users are allowed to access.
- » **Mail server:** A mail server is responsible for sending and receiving email for users within the company.
- » **Authentication server:** An authentication server stores all the usernames and passwords for the network in a database, and is responsible for verifying the username and password of the users when they log onto the network. Before accessing files on a file server or reading email, users typically must authenticate to the authentication server first.
- » **Syslog server:** A syslog server is a central server that all logging activity can be sent to. For example, you can have the logs from your web server and your FTP server sent to a syslog server so that you can monitor the logs at the syslog server. This gives you the benefit of



centralized administration as you do not have to visit the logs of each individual server.

### *Internet appliances and legacy systems*

Servers are not the only types of devices that are found on networks. Networks may also contain a number of appliance devices that provide different functionality to the network. The following is a list of common appliances, or devices, connected to the network:

- » **UTM:** A *Unified Threat Management* appliance is a device that integrates multiple security features into one appliance. UTM typically combines a firewall, an intrusion detection and prevention system, and an antivirus system that checks all incoming data for viruses.
- » **IDS:** An *Intrusion Detection System* (IDS) is a device that monitors network activity and sends out notification when suspicious network activity is detected. The notification could be sent as an email message or as a text message to the administrator's mobile device.
- » **IPS:** An *Intrusion Prevention System* (IPS) is similar to an IDS; however, when it detects suspicious activity it can take corrective action to help prevent the activity from continuing. An example of corrective action would be to deny the system access to the network.
- » **End-point management server:** An end-point management server is a device that pushes out security policies on the network. Client devices such as workstations, laptops, and mobile devices must adhere to these policies before they are allowed to connect to the network.
- » **Legacy/embedded systems:** Networks may also have a number of legacy or older systems present on the network to run older applications that may still be needed by the company.

### *Additional networking terminology*

Another set of terms you will hear when talking with other IT professionals about network concepts is local area network (LAN) and

wide area network (WAN). The following outlines common networking terms you should understand when preparing for the A+ exams:

- » **LAN:** A *local area network* (LAN) is a network that typically involves one office building, or maybe even networked systems on one floor. The major point to remember when identifying a LAN is that there is not a lot of distance between the systems on the network.
- » **WAN:** Comparatively, a *wide area network* (WAN) is a network environment that involves connecting two or more LANs. Each LAN typically covers its own building or office location. Companies typically link each office location to network with the other office locations. Connecting all office locations creates the WAN.
- » **MAN:** A *metropolitan-area network* (MAN) is a network bigger than a LAN but not as big as a WAN environment. The MAN covers a small metropolitan area, while a WAN could cover areas across the country or the world.
- » **PAN:** A *personal-area network* (PAN) is a network created by smaller personal devices typically using Bluetooth.
- » **WMN:** A *wireless mesh network* (WMN) is a group of wireless systems all connected to one another, instead of via a wireless access point. This is a form of wireless ad hoc networking.

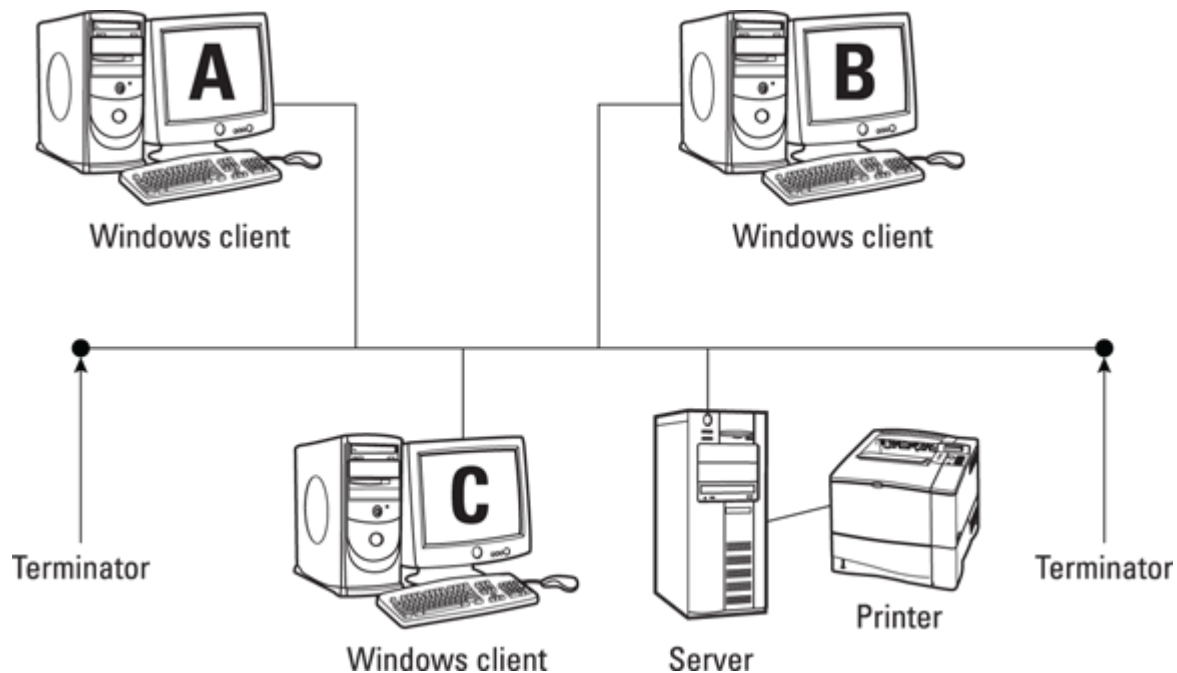
## *Understanding Network Topologies*

When building a network, be cognizant of some upfront decisions regarding the overall network setup. Building a network is like building a database: You have to understand the theory before you start the hands-on work.

*Topology* refers in a general sense to layout; similarly, a *network topology* defines the layout of the network. The three basic network topologies are bus, star, and ring. The following sections discuss the different network topologies and their characteristics.

### *Bus*

A *bus topology* uses a main wire (or trunk) to connect all network devices so that they can communicate with one another. The main trunk is fairly cheap to install but expensive to maintain. [Figure 1-3](#) shows a diagram of a bus topology; notice that all systems are connected to a main cable.



**FIGURE 1-3:** A bus topology.

When a workstation sends data to another workstation in a bus topology, data (in the form of an electrical signal) is delivered across the full length of the trunk. Each workstation looks at all data that runs along the trunk. If the data is destined for a particular workstation, that workstation copies the data to the memory on its network adapter.

For example, [Figure 1-3](#) shows what happens when client A sends information to client B.

1. The information runs along the trunk.
2. When it passes by client C, client C checks whether it is also a destination for the information; if not, client C ignores the data.
3. The information continues down the wire and makes its way to client B.

4. Client B looks at the data to determine whether the data is destined for it; if so, client B copies the data and stores it in the memory on the network card.

Note that because client B has made a *copy* of the data, the data is still on the wire. The data continues on the wire past the server and hits the terminator at the end of the trunk segment.

A *terminator* is a device that absorbs the electrical signal when it reaches the end of the network trunk. If there were no terminator at the end of the cable, the signal would bounce back in the other direction and collide with any new data being placed on the wire. So, to prevent this collision, the terminator grabs any signals that hit it and ensures that it is absorbed off the wire.

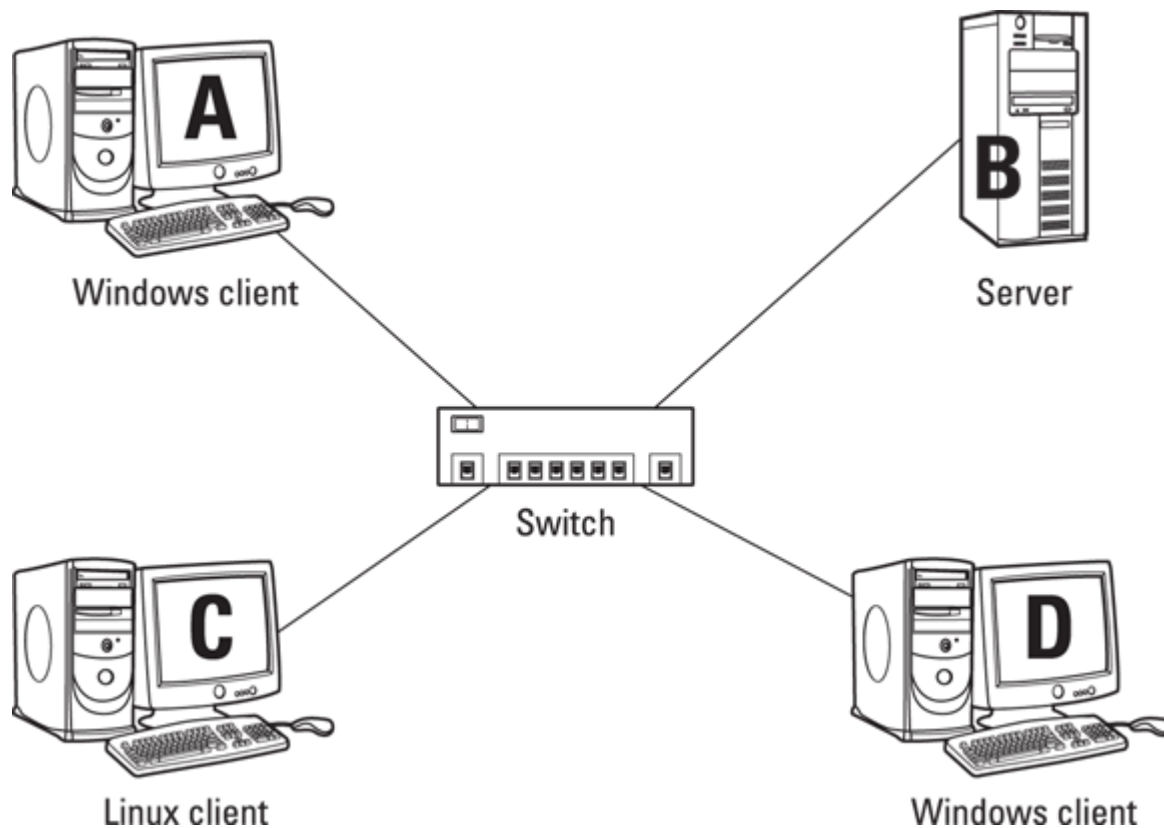


FOR THE  
EXAM

In a bus topology, any break in the wire creates a nonterminated end. When there is a nonterminated end on the bus signal bounce occurs and as a result the entire network collapses.

## *Star*

One of the most popular types of network topologies today is the star topology. A *star topology*, shown in [Figure 1-4](#), involves a central component, called a *hub* (older networks) or a *switch* (today's networks), which connects all systems and is used to send the electrical signal to all connected systems.



**FIGURE 1-4:** A star topology.

With the star topology shown in [Figure 1-4](#), if client A sends information to client D, the information first travels from client A to the hub. The hub sends the information through each port on the hub: as a result, reaching each workstation connected to the hub. Each workstation is responsible for determining whether it is the data's intended destination. When client D receives the data, it checks the destination address of the packet, identifies itself as the recipient of the data, and then copies the data to the network adapter's memory. If the data is not destined for the client, the client simply discards the packet.

Today's networks use switches instead of hubs. Here's an example of how a switch works. When client A sends data to client D, the information first travels from client A to the switch and then the switch forwards the information only to the port that client D resides on. The information does not get sent to all the clients connected to the switch, like what a hub does. This data path offers performance benefits and also security benefits. Find

more on hubs and switches later in the “[Working with Network Devices](#)” section of this chapter.

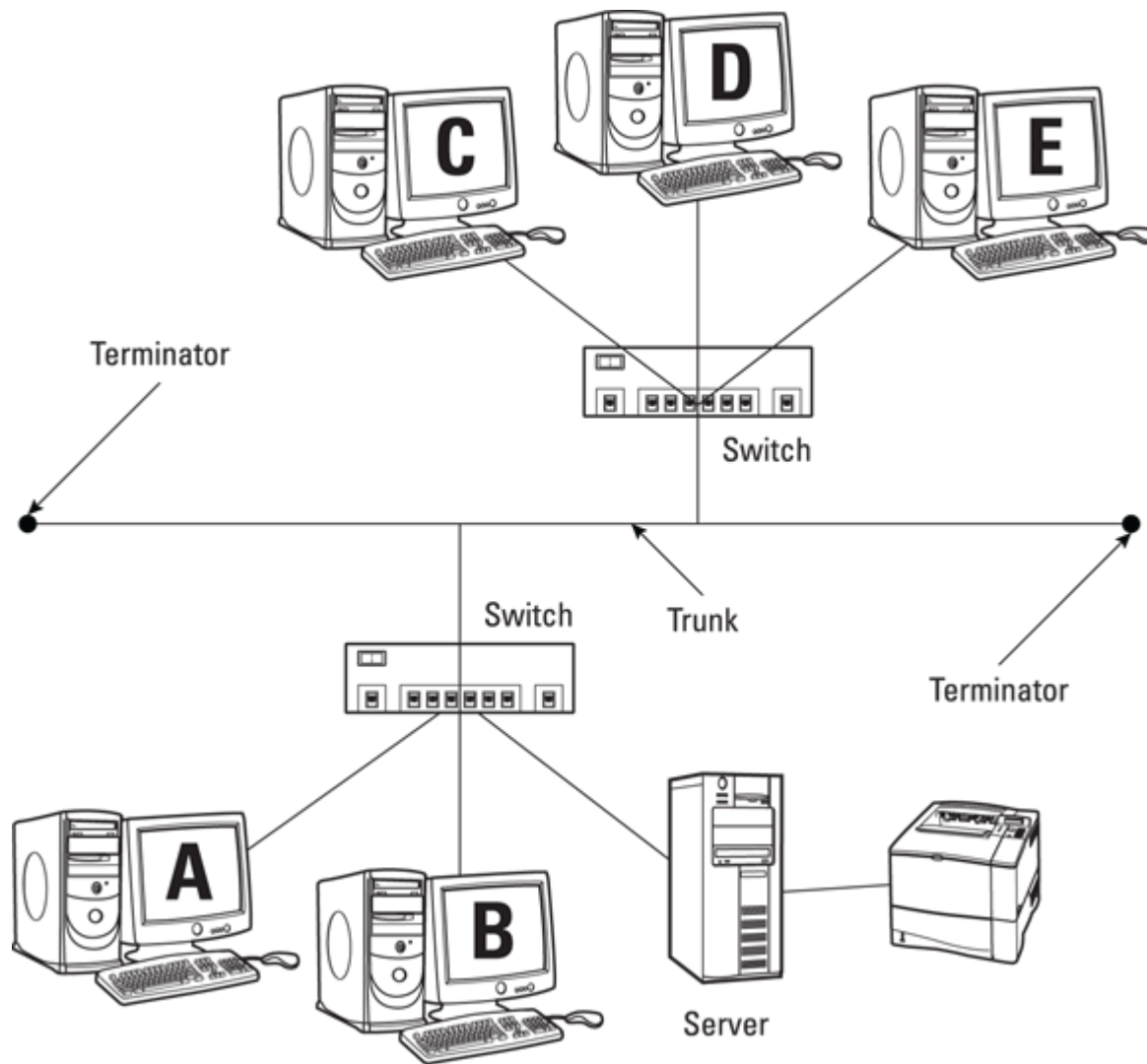
One of the major benefits of using a star topology is that if a cable breaks, it doesn’t take down the entire network like it would with a bus topology; only the workstation connected to the broken cable is affected. If a hub device breaks, however, the entire network fails. In all fairness, though, the cost to implement a star topology might be a little more than a bus topology because of the price of the hub or switch device used.

## ***Mesh***

A *mesh topology* is a network topology that involves each system having a connection to every other system on the network. This is very costly because you need enough equipment such as network cables and network cards to connect all systems to one another. The benefit of a mesh topology is that you have multiple pathways to send data to any system on the network. This is a way to add fault tolerance to the communication system.

## ***Hybrid***

A *hybrid topology* is a mixture of two or all of the three basic topologies. For example, you could use a bus topology as a main trunk, connect hubs to the main trunk, and then connect the systems to the hubs. [Figure 1-5](#) shows an example of this type of hybrid topology.



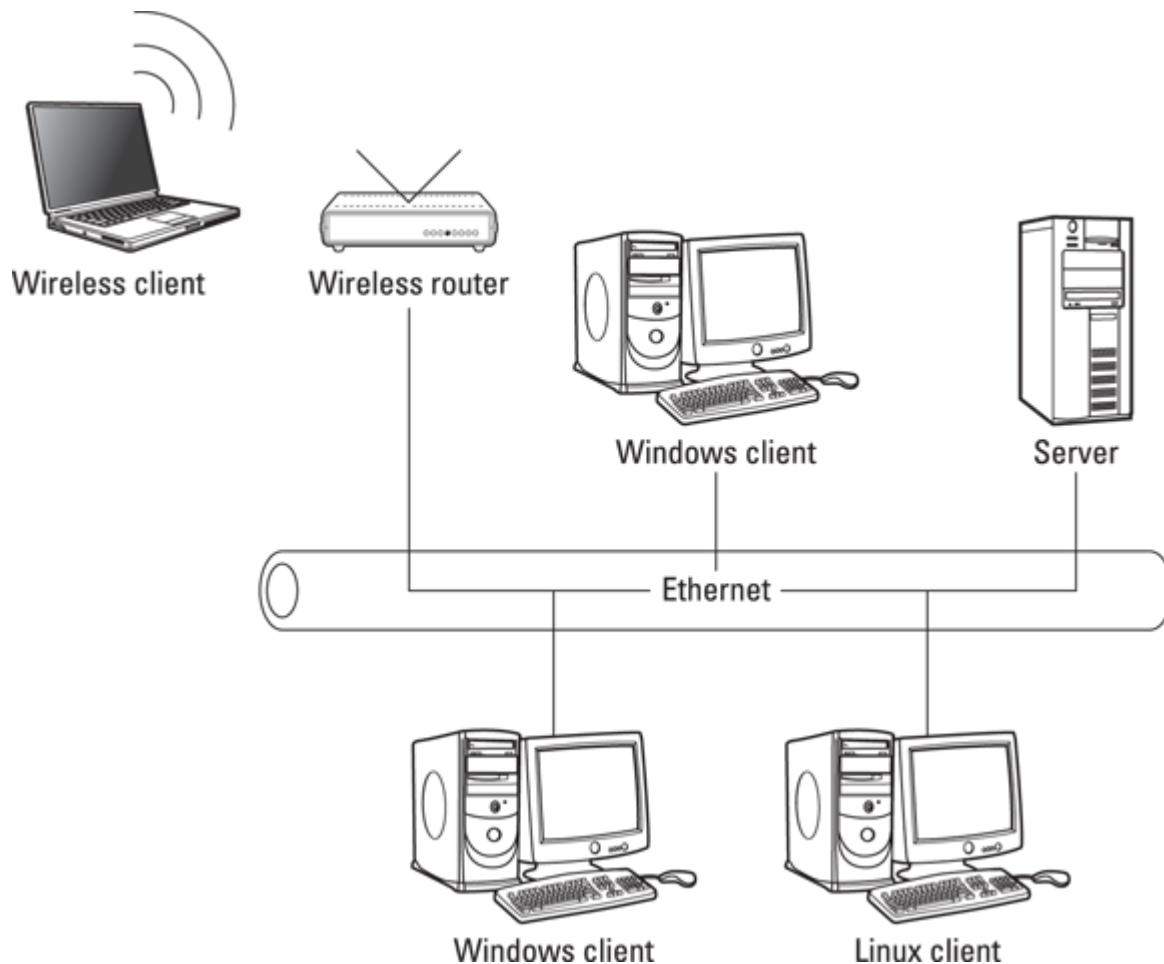
**FIGURE 1-5:** A hybrid topology.

To be more accurate, the configuration shown in [Figure 1-5](#) could be called a *star-bus topology* — a star topology mixed with a bus topology. Today, the most popular topology in use is the star topology — or maybe even a hybrid topology using a star-bus layout.

## **Wireless**

Today's networks allow more mobility for network clients by supporting wireless technologies. To implement a wireless solution, you build a wireless network that uses a wireless topology. A *wireless topology* typically involves a wired network with wireless clients connecting to the wired network through a *wireless access point (WAP)*, which is a device

that sends and receives signals to a wireless client via radio waves (shown in [Figure 1-6](#)).



**FIGURE 1-6:** A wireless network topology.

Notice in [Figure 1-6](#) that the wireless client sends data to the WAP, which has a connection to the wired network. The WAP sends the wireless data to the destination system by sending the signal through the wired media.

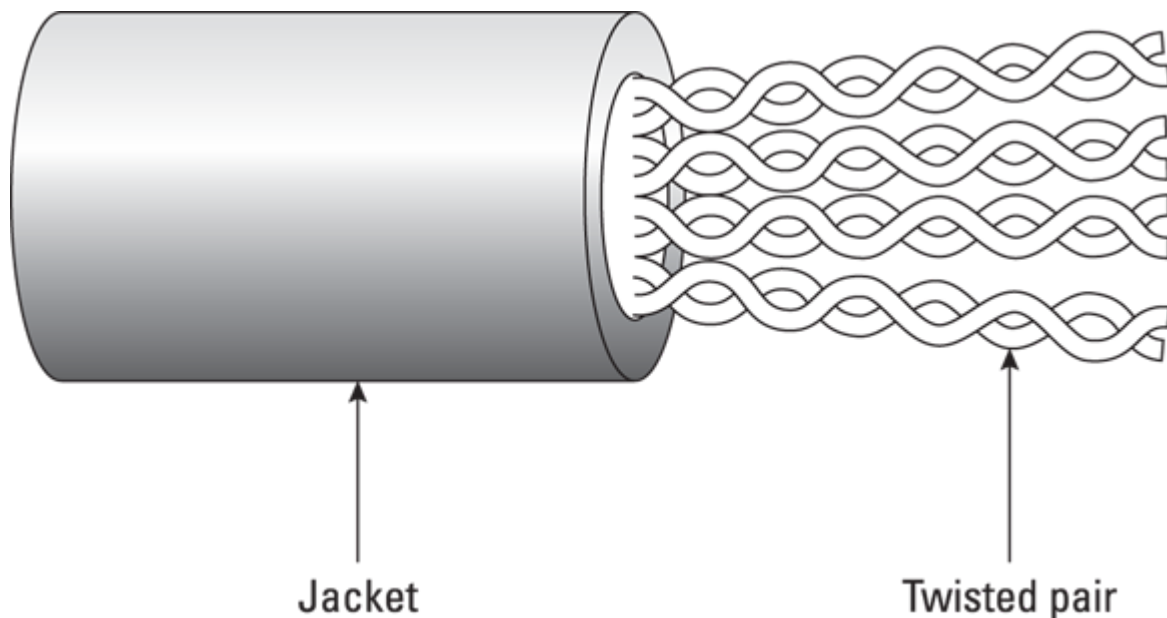
## *Connecting with Network Cabling*

After choosing your network topology, it is time to connect all the network devices together, which means deciding the type of cabling to use. The following sections discuss and evaluate the different types of cabling available for standard networks.

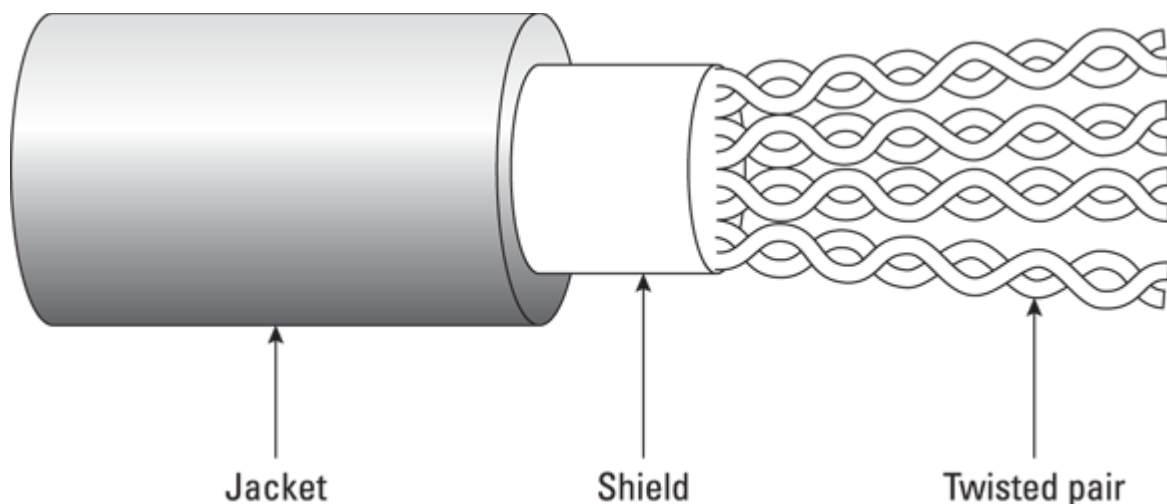


## *Twisted pair*

*Twisted pair cabling*, which is inexpensive and easy to use, is one of the most popular types of cabling used. It gets its name from the fact that it contains four pairs of wires twisted around each other inside the cable's outer *jacket*, the outer covering of the cabling shown in [Figures 1-7](#) and [1-8](#). Twisted pair cabling comes in two variants — unshielded twisted pair (UTP) and shielded twisted pair (STP) — shown in [Figure 1-7](#) and [Figure 1-8](#), respectively.



**FIGURE 1-7:** Unshielded twisted pair cabling.



**FIGURE 1-8:** Shielded twisted pair cabling.

The only difference between UTP and STP is that STP cabling has an extra layer of insulation, which helps prevent interference from outside devices or cabling. Such interference can distort the data traveling along the cable length.

UTP comes in a number of different flavors, called *grades* or *categories*. [Table 1-1](#) lists the categories of UTP cabling, as well as their purpose and speed.

**TABLE 1-1 UTP Category**

<i>Category</i>	<i>Purpose</i>	<i>Speed</i>
Category 1 (CAT1)	Voice only	
Category 2 (CAT2)	Data	4 Mbps
Category 3 (CAT3)	Data	10 Mbps
Category 4 (CAT4)	Data	16 Mbps
Category 5 (CAT5)	Data	100 Mbps
Category 5e (CAT5e)	Data	1 Gbps
Category 6 (CAT6)	Data	10 Gbps
Category 6e (CAT6e)	Data	10 Gbps
Category 7 (CAT7)	Data	10 Gbps

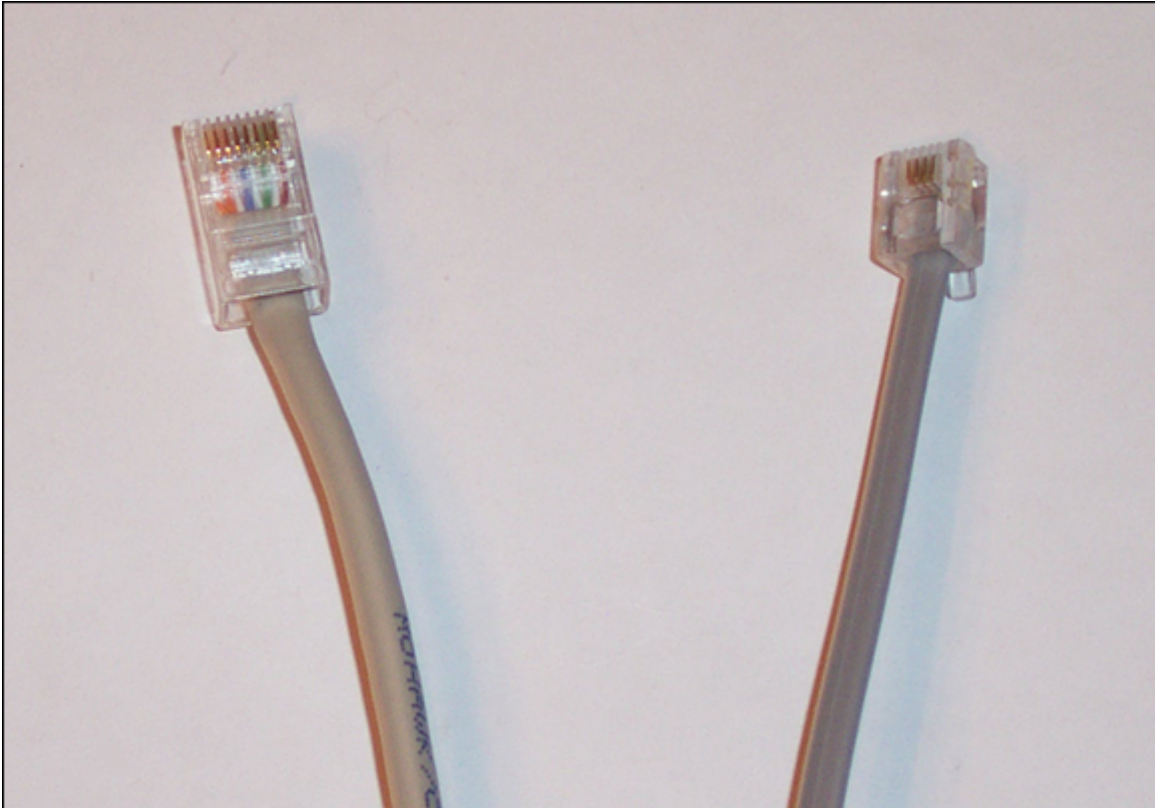
Because twisted pair cabling does not have the layers of shielding found in other forms of cabling, the data is pretty much unreadable — or the integrity of the data is questionable — after 100 meters. For this reason, twisted pair cabling has a maximum length of 100 meters.



**FOR THE  
EXAM**

For the A+ exams, you are expected to know the speeds of the different categories of UTP cabling. Also, remember that twisted pair cabling has a maximum distance of 100 meters regardless of whether it is a shielded or unshielded twisted pair.

Twisted pair cabling uses a special type of connector to connect the cable to the system or network devices. This connector is similar to those used to connect a telephone to a telephone jack. Network devices that use twisted pair cabling use the RJ-45 connector, and telephones use the RJ-11 connector. [Figure 1-9](#) shows both.



**FIGURE 1-9:** An RJ-45 connector (left) and an RJ-11 connector (right).

## *Wiring standards*

When looking at UTP cabling, two common standards have been defined that dictate the order of the wires within the UTP cable known as T568A and T568B. Each of these standards defines the order of the eight wires within the cable and has been developed to give the best-quality transmission.

The order of the wires within the RJ-45 connector when following the 568A standard are as follows (wire 1 is on the left side):

» Wire 1: White/Green Stripe

- » Wire 2: Green
- » Wire 3: White/Orange Stripe
- » Wire 4: Blue
- » Wire 5: White/Blue Stripe
- » Wire 6: Orange
- » Wire 7: White/Brown Stripe
- » Wire 8: Brown

The order of the wires within the RJ-45 connector when following the 568B standard are as follows (wire 1 is on the left side):

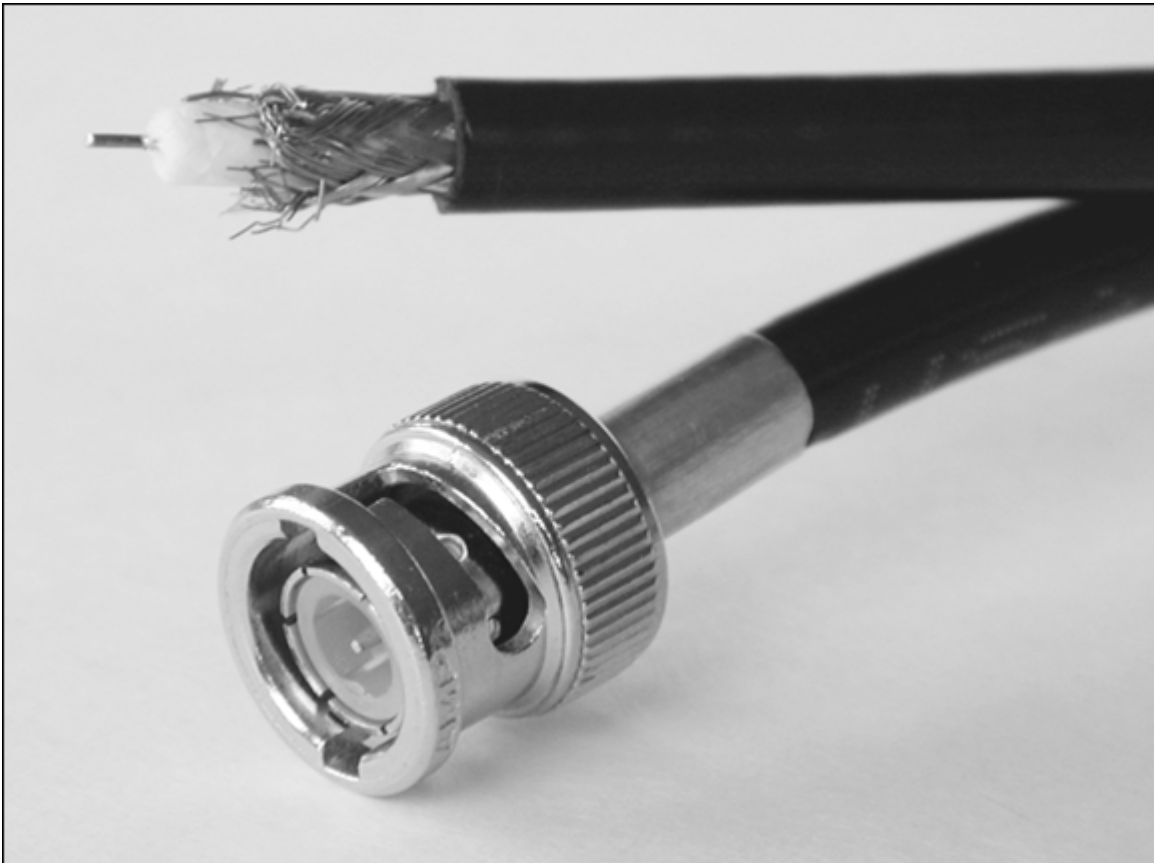
- » Wire 1: White/Orange Stripe
- » Wire 2: Orange
- » Wire 3: White/Green Stripe
- » Wire 4: Blue
- » Wire 5: White/Blue Stripe
- » Wire 6: Green
- » Wire 7: White/Brown Stripe
- » Wire 8: Brown

Note that to create a straight-through cable you wire both ends using the same standard, while to create a crossover cable (used to connect two devices directly together without using a switch) you wire one end as 568A and the other end as 568B. This is essentially changing the transmit and receive wires so that the two stations can talk directly. The reason to choosing 568A or 568B is strictly to help define whether you are creating a straight-through or crossover; there is no performance or security benefit of one or the other.

## *Coaxial*

*Coaxial (coax) cabling* is the type of cable you use for cable television. A copper wire in the center of the cable is responsible for transmitting

information. Furthermore, the copper wire is protected by two levels of insulation and an exterior plastic covering, as shown in [Figure 1-10](#).



**FIGURE 1-10:** Looking at coaxial cable and a coax cable with the BNC style connector.

Like UTP, coaxial cabling used for networking comes in different flavors — two, to be exact. *Thinnet* is only one-quarter-inch thick, and *Thicknet* is one-half-inch thick. [Table 1-2](#) shows the difference between Thinnet and Thicknet.

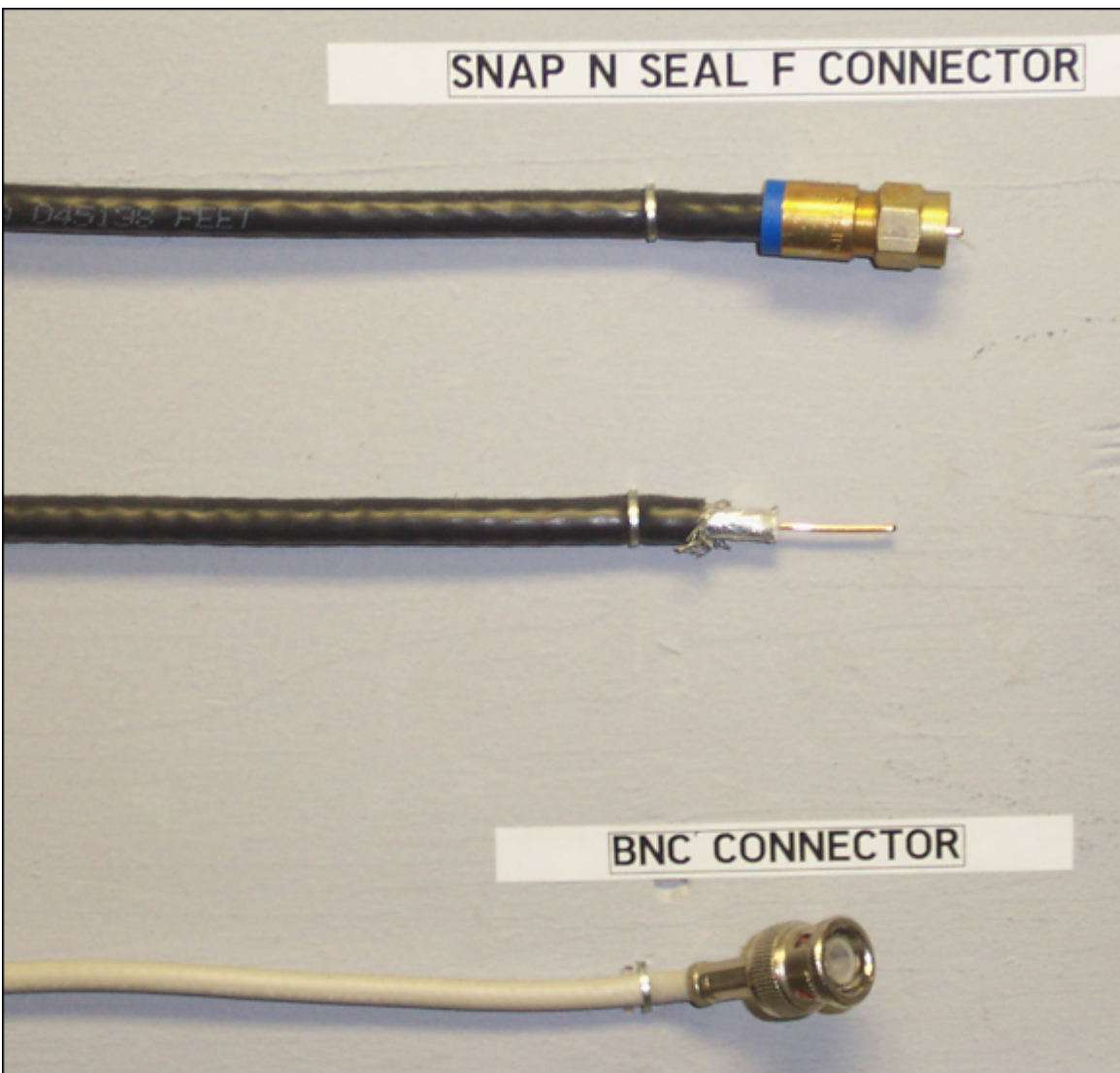
**[TABLE 1-2](#) Types of Coax Cabling**

Type	Coax Type	Maximum Cable Length	Diameter	Speed
Thinnet	RG-58	185 meters	¼"	10 Mbps
Thicknet	RG-8	500 meters	½"	10 Mbps

Notice in [Table 1-2](#) that the coaxial cable type is specified by a *radio grade (RG)*. There are a number of grade standards for coaxial cable, and

each standard has a specific purpose and connector type that will work with that type of cabling. For example, RG-58—grade cabling (Thinnet) uses BNC connectors (discussed in more detail in the next section), and an RG-8—grade cable uses an AUI connector.

Another popular grade of coaxial cable is RG-6 — the grade of coax used for television cable — which uses the F-type connector (also known as the *F-connector*) to connect the cable to the device. [Figure 1-11](#) displays coaxial cables along with an F connector and a BNC connector. Another common-grade coax cable that is used by cable television is RG-59.



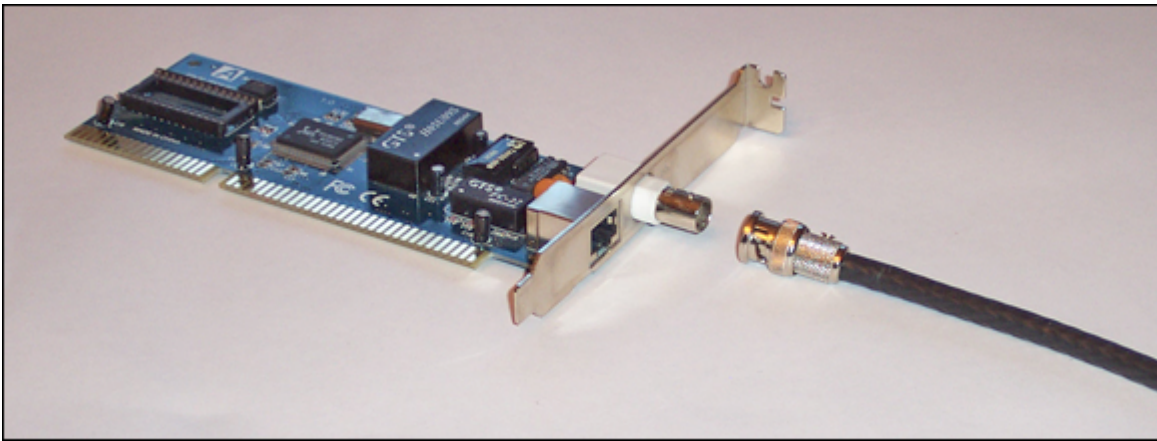
**FIGURE 1-11:** An F-type connector and a BNC connector.



## *Connecting with Thinnet*

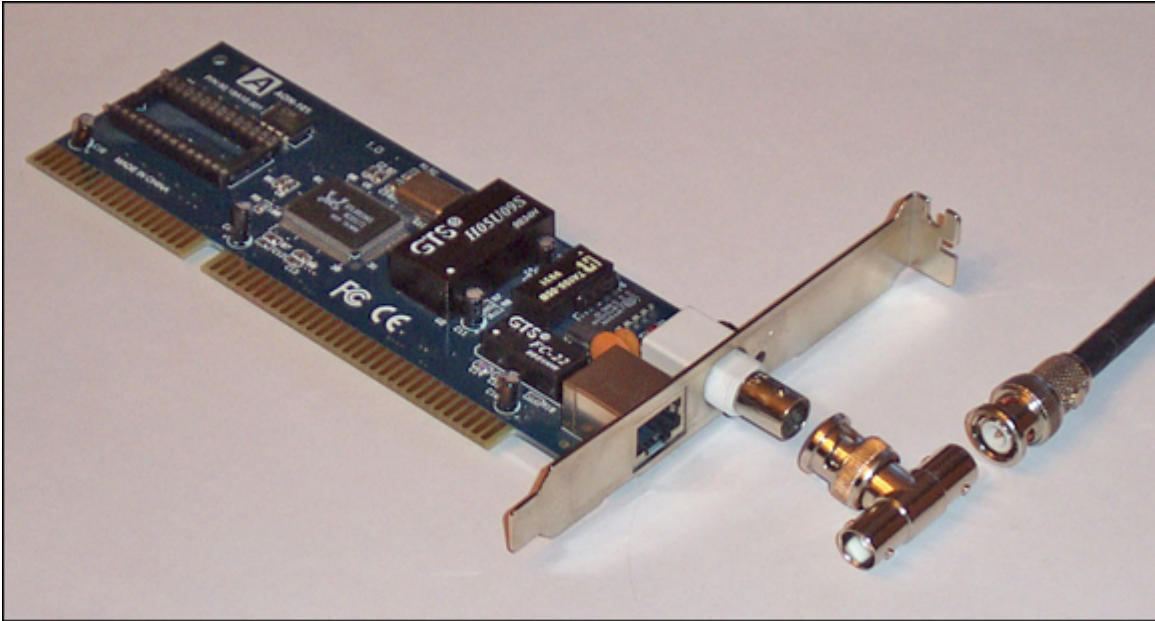
When using Thinnet to connect to a workstation, you need to use a *Bayonet Neill-Concelman* (BNC) connector — also known as British Naval Connector (BNC), which comes in a few forms. You will most likely encounter the plain old BNC and the BNC-T.

The BNC connector connects Thinnet cable to a networking device, such as a network card, using the barrel connector on the back of the network card, as shown in [Figure 1-12](#).



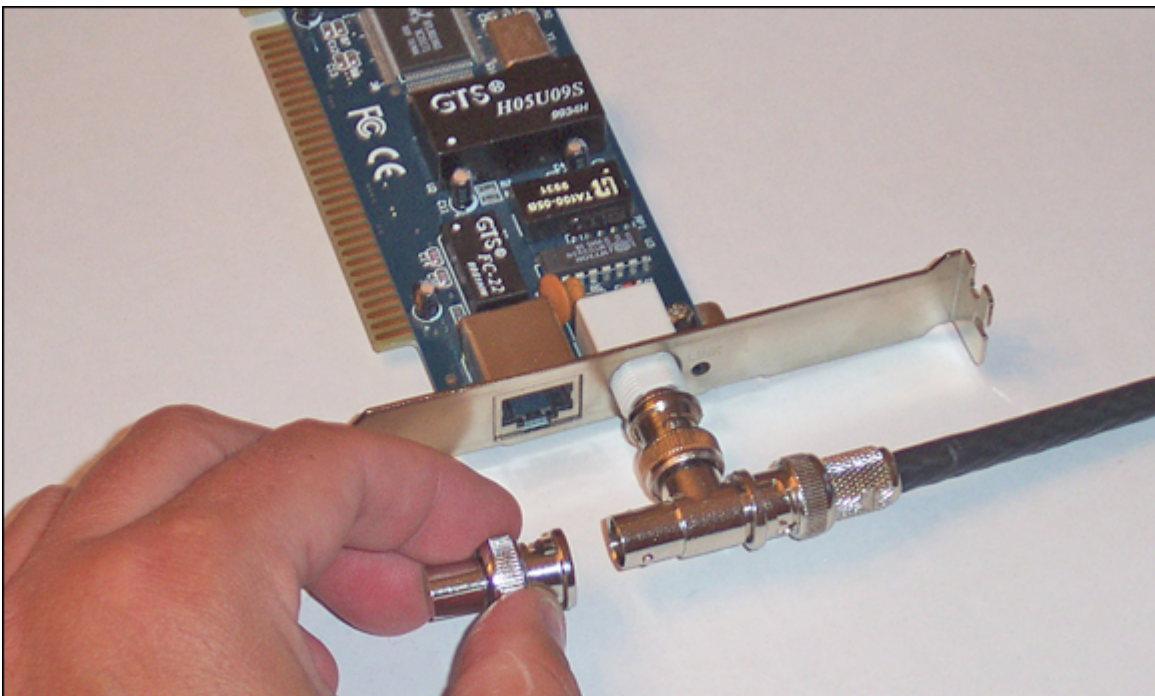
**FIGURE 1-12:** A BNC connector connecting to a workstation.

The BNC-T — shaped like the letter *T* — is used to continue the cable length while “T-ing” off to connect a system to the network, as shown in [Figure 1-13](#).



**FIGURE 1-13:** A BNC-T connector used on Thinnet coax cable.

Notice in [Figure 1-14](#) that the BNC-T connects to a metal barrel-type port on the back of the network card. If you do not need to continue the cable length and this is your last workstation, you are required to terminate the end with a terminator on the T connector, as shown in [Figure 1-14](#).

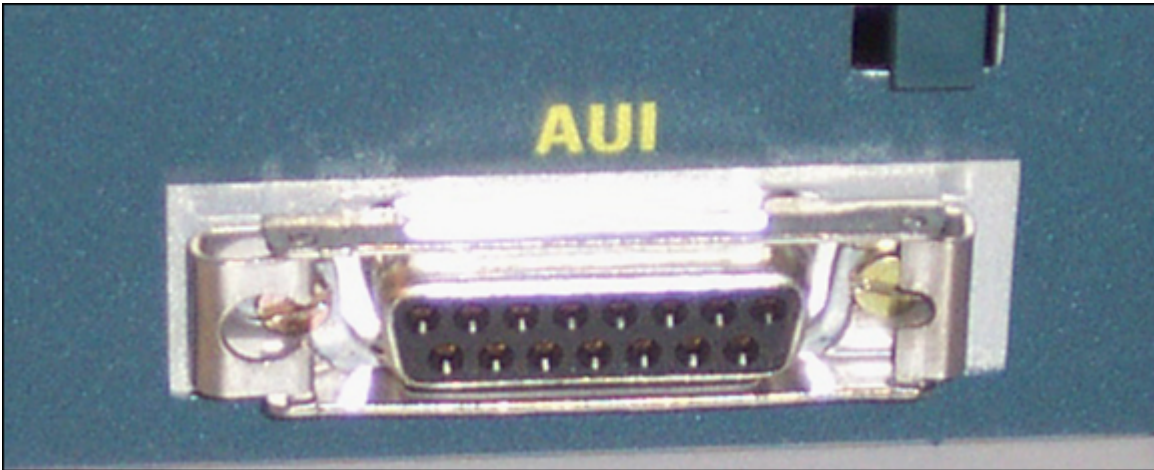


**FIGURE 1-14:** A BNC-T connector with a terminator.



## Connecting with Thicknet

A system or device connected to a Thicknet network uses an *adapter unit interface (AUI)* port (shown in [Figure 1-15](#)), which connects the system to the Thicknet cabling by using a transceiver known as a *vampire tap*.



**FIGURE 1-15:** An AUI port.



TECHNICAL  
STUFF

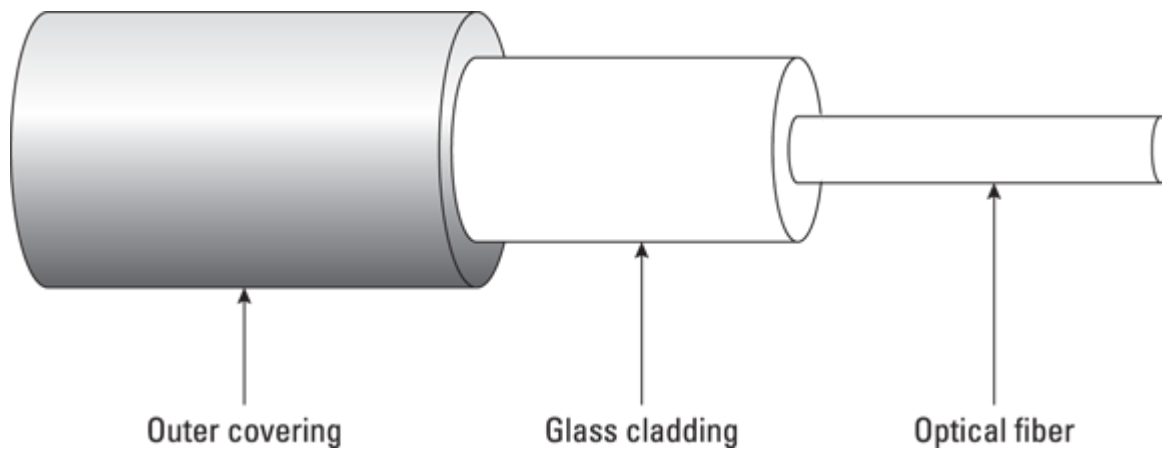
The vampire tap gets its name by having small “teeth” that clamp to the cable and cut into the cable’s core, allowing the electrical signal to travel from the system to main network cable and beyond.

Although older network environments such as Thinnet and Thicknet used coaxial cable, coaxial is still used today with broadband (high-speed) Internet connections by the cable companies. The Internet connection comes into my home via a coaxial cable and then connects to a cable modem, which my router is connected to, to give Internet to the entire house.

## Fiber optic

Fiber optic cabling — one of the fastest types of network media available — is made of a glass fiber core (optical fiber) surrounded by a layer of glass cladding insulation that is then covered with an outer covering (jacket). There are two fiber channels in fiber optic cable: one for

sending information and the other for receiving information. [Figure 1-16](#) illustrates a fiber optic cable.



**FIGURE 1-16:** Fiber optic cabling.

Fiber optic cabling can reach distances of 2 kilometers (km) or more, carrying a signal for a much greater distance than twisted pair and coaxial cabling. Fiber optic cabling is also fast, transmitting information at speeds of 1 Gigabit per second (Gbps) and higher. And, because fiber carries data in pulses of light instead of electronic signals, data cannot be corrupted by outside electronic interference.



**FOR THE  
EXAM**

You will be expected to know details regarding fiber optic cabling for the A+ exams. Fiber carries data through pulses of light along its glass core and can reach distances of 2 km. Fiber optic cable transmits information at speeds that range from 100 Mbps to 10 Gbps.

The two implementations of fiber optic cabling are single-mode fiber (SMF) and multi-mode fiber (MMF):

- » **Single-mode fiber (SMF):** Uses only one ray of light, known as a *mode*, to carry the transmission over great distances.
- » **Multi-mode fiber (MMF):** Takes advantage of multiple rays of light, or modes, simultaneously. Each ray of light runs at a different

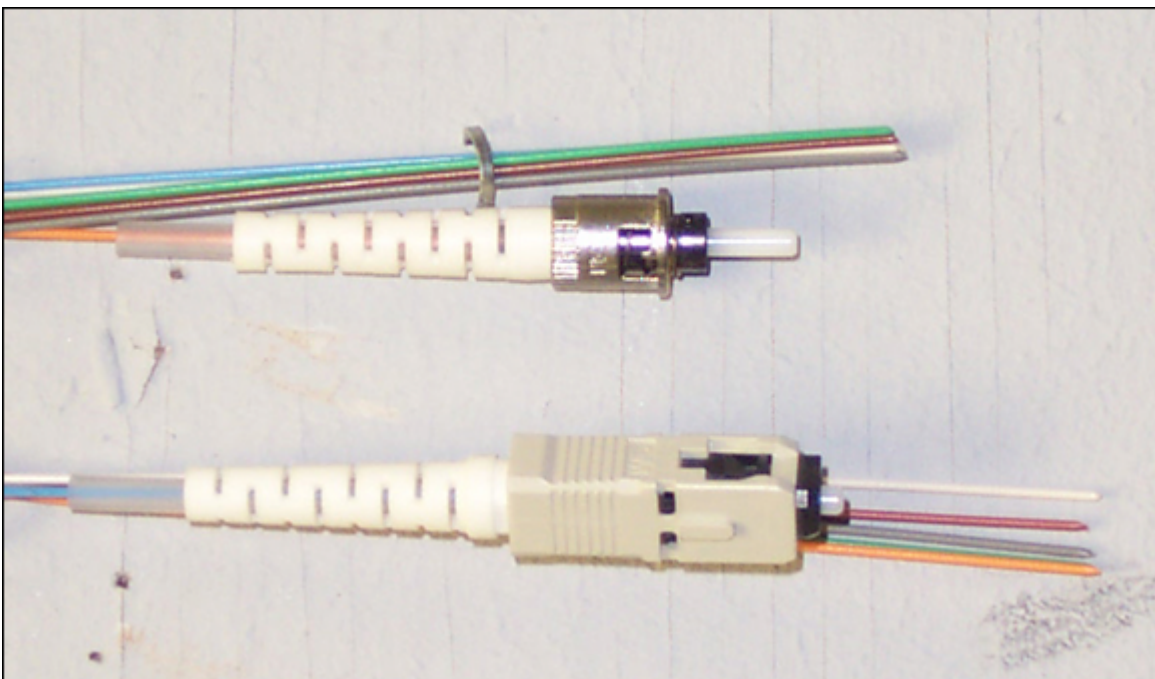
reflection angle and is used to transmit data over short distances.



FOR THE  
EXAM

Fiber optic cabling uses a number of different types of connectors. The following list provides a few that you need to be familiar with for the A+ exams:

- » **Straight tip (ST):** The straight tip connector is derived from the BNC-style connector but uses a fiber optic cable instead of the copper cabling used with BNC. [Figure 1-17](#) shows an SC and ST connector.
- » **Subscriber connector (SC):** The subscriber connector is rectangular and is somewhat similar to an RJ-45 connector.
- » **Fiber local connector (LC) and mechanical transfer-registered jack (MT-RJ):** These newer fiber optic connector types resemble the registered jack and fiber SC shape. The MT-RJ is a small connector similar in appearance to an RJ-45 connector. The LC is similar in appearance to the fiber SC connectors and is the preferred connector for transmissions exceeding 1 Gbps because of its small form factor.



**FIGURE 1-17:** Looking at strands in fiber optic cabling along with the SC (bottom) and ST (top) connectors.

The primary disadvantages of using fiber optic cabling are the implementation cost and the expertise required for the wiring.

## *Troubleshooting Networking Cables*

Most network professionals use cable testers to test the cabling and verify that the cable is properly crimped and making contact with the networking devices. For example, cable testers for CAT5 cabling identify whether each of the eight wires is crimped properly and identify other problems, such as wires being crimped in the wrong order.

### *EMI*

Another problem you need to be aware of when running cable throughout a building is that twisted pair and coaxial cables are susceptible to outside interference from other electrical components. For example, do not put networking cable alongside the electrical cabling because the electrical cabling could cause interference that could make the data on the network cable unreadable. For more information on cable testers and troubleshooting cabling problems, check out Book 4, [Chapter 2](#).

### *Plenum*

Here is one last point to make about cabling to help you prepare for the A+ certification exams. *Plenum* — the space between the ceiling tile and the floor above — is a popular place to run cables. If you are going to run cables in this area, make sure that you are use plenum-grade cabling, known as Teflon-covered cable. If you are using nonplenum-grade cabling, such as PVC cover cabling, in this space and a fire happens, the PVC coating can give off a toxin that could be spread throughout the building.

### *Splitter and signal quality*

It is common to want to split a signal travelling through a cable in order to send that signal to multiple places, such as to send the cable signal for one

TV to an additional TV. There are a number of different types of cable splitters that correspond to the different cable types. For example, to split your TV signal you need a coaxial cable splitter. It is important to note that when you split the cable this way, you lose signal quality due to the fact that the power carrying the signal is split as well. The less power, the weaker the signal.

## *Examining Network Access Methods*

*Network access* refers to the different methods that computers use to place data on the network. This section discusses these methods and identifies the advantages and disadvantages of each.

### *CSMA/CD*

One of the most popular types of access methods is CSMA/CD (Carrier Sense Multiple Access/Collision Detection). Understanding this term is easier if you break it down into its individual parts and examine each part in detail:

- » **Carrier sense:** All computers on the network are watching, or sensing, the network for network traffic. If the network has data already on the wire, a system will wait until the wire is free of traffic.
- » **Multiple access:** All computers on the network have equal access to the network at any given time. In other words, anyone can place data on the network whenever he or she chooses. Note, however, that workstations on the network will try not to place data on the wire at the same time the wire is transmitting other data because the two pieces of data will collide, destroying the data. That's why it's so important for workstations to "sense" the wire.

To summarize, *carrier sense multiple access* suggests that all workstations have access to the network and are watching the network to make sure it is clear of data before they send out their information.

» **Collision detection:** When two workstations send information at the same time, the data will collide and be damaged in transit. When two workstations have data that has been involved in a collision, they resend the information out on the network at variable intervals to prevent the data from colliding again.

The nice thing about CSMA/CD is that the workstations decide when to send data, trying to prevent collisions. However, there is always the possibility that multiple workstations will send data out at the exact same moment the network is clear, resulting in data collision.

## CSMA/CA

Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) is similar to CSMA/CD except for one main difference: When a workstation senses that the wire is free, it sends out dummy data first instead of real data. If the dummy data collides with other information on the wire, the workstation has avoided a collision with the real data; if the dummy data does not collide, then the workstation sends the real data. Like CSMA/CD, if the real data collides and does not reach its destination, it will be resent by the sender.

CSMA/CA is used with 802.11 wireless networking.

# *Piecing Together the Network Architectures*

A *network architecture* describes a network technology that uses a specific topology, cable type, and access method. This section describes the major types of architectures and their characteristics.



**REMEMBER** Many people use the term *architecture* to mean *topology*, stating that the three main types of architectures are bus, star, and ring. However, bus, star, and ring are properly defined as topologies, not

architectures. Be careful not to confuse the two terms. A *topology* defines the network layout, whereas an *architecture* is made up of a topology, cable type, and access method.

## ***Ethernet***

*Ethernet* is probably the most popular type of network architecture in use. Ethernet is an example of a network architecture that comes in multiple flavors. If someone says to you, “I have an Ethernet network,” you are likely to ask, “What type of Ethernet?”

There are a number of types of Ethernet: 10BaseT, 10Base2, 10Base5, 100BaseT, and 1000BaseT being a few popular ones. All Ethernet architectures use CSMA/CD as the access method, but each type of Ethernet uses a different topology or cable type. The following sections outline the differences among them.

### ***10 Mbps Ethernet standards***

The following outlines some of the popular 10 Mbps network architectures that have been popular in past years. You need to be familiar with these for the A+ exams:

- » **10BaseT:** A network architecture that typically uses a star topology but can, in some cases, use a hybrid star-bus topology. 10BaseT networks primarily use CAT3 UTP cabling, which transfers information at 10 Mbps. 10BaseT uses the CSMA/CD access method for putting information on the network.
- » **10Base2:** A network architecture that uses a bus topology, but can sometimes use a hybrid star-bus topology. 10Base2 networks typically use Thinnet coaxial cabling, which transfers information at 10 Mbps. 10Base2 uses CSMA/CD as its access method.
- » **10Base5:** A network architecture that uses a bus topology. 10Base5 networks primarily use Thicknet coaxial cabling, which transfers information at 10 Mbps. Like 10Base2, 10Base5 uses CSMA/CD as its access method.
- » **10BaseFL:** An old Ethernet architecture that ran at 10 Mbps and used fiber optic cabling. 10BaseFL uses CSMA/CD as the access method.

## ***100 Mbps Ethernet standards***

You are unlikely to see a 10 Mbps network architecture on today's networks, so it is more important that you have an idea of some of the popular 100 Mbps Ethernet architectures:

- » **100BaseT:** An improved network architecture over the 10BaseT networks. It uses a star topology, but can also be found using a hybrid star-bus topology. 100BaseT networks primarily use CAT5 UTP cabling, which transfers information at 100 Mbps. 100BaseT also uses CSMA/CD as its access method.
- » **100BaseFX:** Another Ethernet architecture that runs at 100 Mbps but is different than 100BaseT in that it uses fiber optic cabling instead of UTP cable. 100BaseT and 100BaseFX are referred to as the “Fast Ethernet” standards. 100BaseFX uses CSMA/CD as the access method.



**TIP** When trying to remember the names of these network architectures, start by looking at the number at the beginning of the name — it indicates the transfer rate. In these cases, the transfer rate is 100 Mbps. You can then look at the tail end of the name to tell what type of cable the architecture uses. For example, in 100BaseT, the letter “T” at the end of the name implies “twisted pair.” The word “base” in the middle means *baseband transmission*, which means that the signal takes up the entire width of the media when sending and receiving data.

## ***Gigabit Ethernet standards***

Today's corporate networks are reaching 1 Gbps (1000 Mbps) and higher, so it is important that you are familiar with the Gigabit Ethernet standards for the A+ exams:

- » **1000BaseT:** Uses UTP cabling; uses CSMA/CD as the access method



- » **1000BaseSX:** Uses multimode, fiber optic cabling for short distances; uses CSMA/CD as the access method



**TIP** Remember this architecture by the *S* in the name, meaning *short* distances.

- » **1000BaseLX:** Uses single-mode fiber optic cabling; uses CSMA/CD as the access method



**REMEMBER** Because single-mode fiber optic cabling is designed for long distances, it is the type of fiber optics used for 1000BaseLX. Remember this standard by the *L* in the name, implying *long* distances.

## 10 Gbps Ethernet standards

Some of the fastest network standards today fall into the 10 Gbps Ethernet architectures. The 10 Gbps Ethernet architectures use fiber optic cabling, either SMF or MMF, depending upon the architecture. For example, the 10GBaseSR standards uses multimode fiber optic cabling that can reach a short distance of 100 meters, and 10GBaseLR uses single-mode fiber optic cabling that reaches a distance of 10 km.



**TIP** Nowadays, you will probably purchase network cards that are marketed as 10/100 cards or maybe even 10/100/1000 cards. This means that the network card can be used with networking environments that transfer information at 10 Mbps, 100 Mbps, or 1000 Mbps.



**ON THE WEB**

Lab 1-1 helps you review the different network architectures. You can find Lab 1-1 on the companion website at

# Understanding Network Protocols

To ensure that all the networking components work with one another, networking standards have been developed. If a company decides that it wants to develop something like a network card, it will ensure that the network card follows a standard so that it can communicate with all the other networking components. In this section, you find out about the different network standards that help each networking vendor develop networking components that function alongside other networking devices.

## IEEE standards

The *Institute of Electrical and Electronics Engineers (IEEE)* has developed a number of LAN standards that define the physical components of networking technologies. In these standards, the IEEE has defined such things as how network cards place data on the wire and the type of cabling used in different types of LANs. The LAN standards are defined by Project 802, which was launched in February 1980. These 12 standards, shown in [Table 1-3](#), define different networking architectures.

**TABLE 1-3 Project 802 LAN Standards**

Project	Description
802.1	Internetworking
802.2	Logical Link Control (LLC)
802.3	Ethernet (CSMA/CD)
802.4	Token Bus LAN
802.5	Token Ring LAN
802.6	Metropolitan Area Network
802.7	Broadband Technical Advisory Group
802.8	Fiber Optic Technical Advisory Group
802.9	Integrated Voice/Data Network
802.10	Network Security

<b>Project</b>	<b>Description</b>
802.11	Wireless Networks
802.12	Demand Priority Access LAN

A few of the networking standards that you should be familiar with are 802.3, 802.5, and 802.11:

- » **802.3:** This networking standard defines the Ethernet architecture, also known as CSMA/CD. This standard defines how data is placed on the wire. A system senses the wire to verify that it is free of data and then submits the data.
- » **802.5:** This IEEE standard defines the token ring network architecture. This architecture uses the token passing access method, which is a set of rules that control how a system submits data on the wire.
- » **802.11:** This IEEE standard defines wireless networking. Wireless networking has evolved over the past few years, and as a result, there are a few different types of wireless networks, wireless 802.11b and 802.11g being the two dominant standards:
  - *802.11b*: This wireless standard has a transfer rate of 11 Mbps and runs at the 2.4 GHz frequency range. 802.11b created the WiFi standard.
  - *802.11g*: This wireless standard has a transfer rate of 54 Mbps and is backward compatible with 802.11b because it also runs at the 2.4 GHz frequency and is part of the WiFi standard. This means that you can have an 802.11b WAP and have a system with a more current 802.11g wireless network card, and both systems will still be able to communicate. They will use the lower transmission rate of the two, though!
  - *802.11n*: This new wireless standard has a transfer rate of up to 300 Mbps and is compatible with 802.11b and 802.11g wireless networking environments because it runs at the 2.4 GHz frequency.



FOR THE  
EXAM

For the A+ exams, you don't need to memorize the entire list of standards. However, know that Ethernet is defined in Project 802.3, token ring is defined in Project 802.5, and 802.11 defines the wireless standards. You will be tested on them!

For more information on wireless networking, check out the next chapter.

## *The OSI model*

The *Open Systems Interconnect (OSI)* model is a seven-layer model defined by the International Standards Organization (ISO) that provides a framework that manufacturers of networking components can use to develop networking hardware and software components.

Each layer of the OSI model is responsible for specific network functions. For example, the network layer is responsible for logical addressing, so any devices or protocols that provide logical addressing run at this layer — such as the IP protocol. [Table 1-4](#) outlines the seven layers of the OSI model and provides examples of networking components that run at that layer.

**TABLE 1-4 The OSI Model**

<i>Layer</i>	<i>Description</i>
7, Application	Responsible for making or receiving a network request and is typically the networking software. For example, a web server, FTP server, and DNS server run at this layer.
6, Presentation	Responsible for formatting the information so that the information is understood on the receiving system. Examples of formatting are compression and encryption.
5, Session	Responsible for opening, closing, and managing a connection (a <i>session</i> ) to another system or device.
4, Transport	Responsible for breaking the information down into smaller pieces so that it can be sent along the network in parts. This layer is also responsible for ensuring that the information reaches the destination.

<b>Layer</b>	<b>Description</b>
3, Network	Responsible for routing of information and logical addressing. A router runs at this layer, and the IP protocol runs at this layer, which provides a logical address (IP address).
2, Data Link	Prepares the information to hit the physical network by placing the data into packets. The data link layer also provides the physical addressing (MAC address), so any device that works with a MAC address runs at this layer (such as a network card, switch, and bridge).
1, Physical	Deals with the network media such as cabling and connectors. The physical layer is also responsible for sending the electrical signal on the wire. Any device that works with the electrical signal runs at this layer such as a hub or repeater.



**FOR THE  
EXAM**

Although the OSI model is more of a Network+ topic, you might receive a few questions on the OSI model with your A+ exams. Be familiar with what layer of the OSI model a hub, switch, and router run at.

## ***Voice over IP (VoIP)***

Voice over IP (VoIP) is a fairly hot topic these days. VoIP deals with allowing subscribers to the VoIP service to have telephone conversations over a TCP/IP network, such as the Internet. The benefit of such a service is no more long-distance charges — just your monthly subscription to the service.

VoIP not only allows for the transmission of voice but also other types of data, such as video. VoIP has become a popular method of communication that supports PC-to-PC communication, essentially using the PC as a phone.

## ***Working with Network Devices***

A computer network is a lot more than just a few computers and a tangle of cables. A computer network needs a number of different types of

devices to connect the systems or to connect the network to another network. This section identifies the different types of network devices popular in network environments today and covers the devices you will be tested on for the A+ exams.



FOR THE  
EXAM

Be familiar with these devices for the A+ exams and understand their benefits.

## *Network interface card (NIC)*

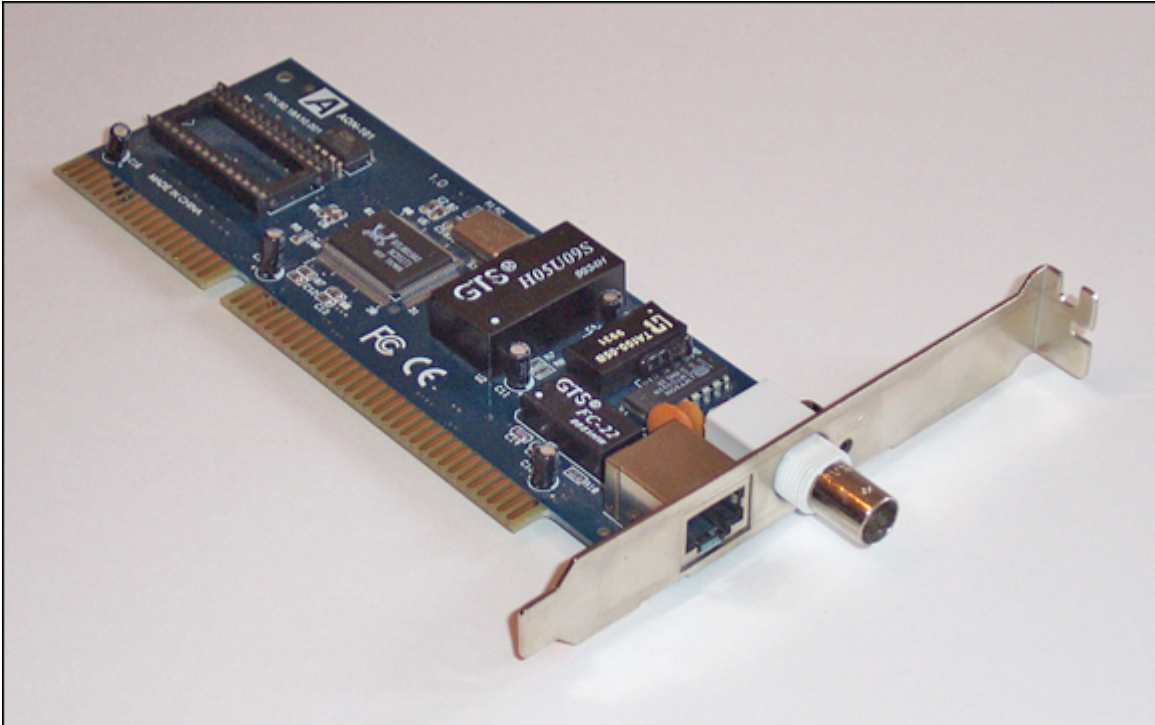
The network interface card (commonly referred to as a *network card*) is responsible for connecting the computer or device to the network. More importantly, the network card on the sending computer is responsible for converting digital data into an electrical signal for copper or optical signal for fiber that can be placed on the wire. The network card on the receiving computer is responsible for picking up the electrical signal and then converting it back to digital data that can be understood by the computer system.

Each network card has a unique address burned into the ROM chip on the card. This unique address is considered the *hardware address* of the network card because the manufacturer of the card burns it into the card. The address uniquely identifies your system on the network. The hardware address is also known as the *Media Access Control (MAC) address*. An example of a MAC address is 00-20-3F-6B-25-13.

Looking at the example of a MAC address, notice that the MAC address is made up of hexadecimal addresses — not your typical decimal numerals or binary values. Of the six groups of digits, the first three pairs identify the manufacturer of the network card, and the last three pairs are a unique set of digits assigned to a particular card built by the manufacturer. So, 00-20-3F, which appears at the beginning of my example MAC address, represents the manufacturer of the card, and 6B-25-13 identifies the card.

The MAC address of the sending and receiving system is stored in the header of the network packet that travels the network wire. When each

system sees the packet traveling by it, it looks at the destination MAC address to decide whether the data is destined for it. If a system finds that it is the intended recipient for the data, it copies the data to its *buffer*, which is memory used to store the information while it waits to be processed. [Figure 1-18](#) shows a network interface card.



**FIGURE 1-18:** A network interface card.



**FOR THE  
EXAM**

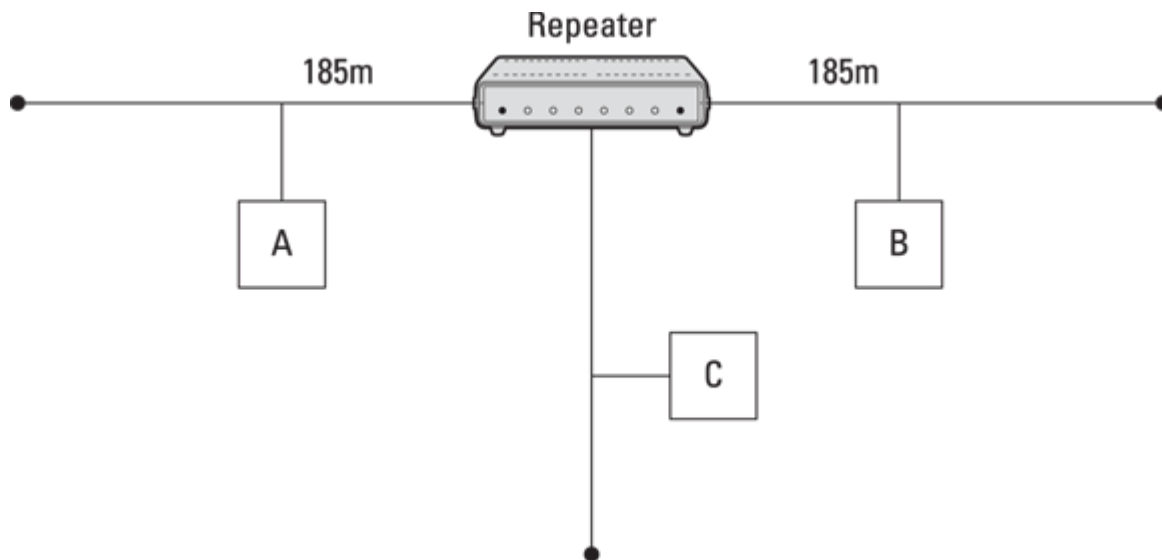
Two lights on the network card act as status indicators — the activity light and the link light. The link light is always lit when you have a connection to the network; the activity light blinks when the network card is sending or receiving information. When troubleshooting network problems, always check that the link light is on, indicating a connection to the network.

## ***Repeater/Extender***

One major concern with cabling is the maximum usable length of the cable. For example, UTP cabling has a maximum length of 100 meters,

and Thinnet has a maximum length of 185 meters. The reason for putting a maximum distance on cable lengths is that the signal traveling along the cable becomes too weak to read at the destination system by the time the maximum length is reached. The term for reduced strength in the signal is attenuation. The receiving computer cannot read the information, and thus does not acknowledge that it received the data. When the sending computer does not receive an acknowledgment, it simply resends the data. This causes the information to be resubmitted, generating more network traffic.

One way to increase the distance of a cable length is to use a *repeater*, which regenerates a signal so it can travel the extra distance. For example, the repeater shown in [Figure 1-19](#) joins two lengths of Thinnet coaxial cable. It joins the two cable lengths so that the signal can travel the distance from computer A to computer B. Note that this distance exceeds 185 meters, which is the maximum distance of Thinnet. When the signal hits the repeater, the repeater rebuilds the signal so that it can travel another 185 meters.



**FIGURE 1-19:** A repeater is used to regenerate the signal.

An *extender* is a device that you can use to connect two cable lengths together to create a much longer cable length. The problem with an extender is that it does not reamplify the signal, so be careful not to exceed the cable length for the type of cable you are extending. For

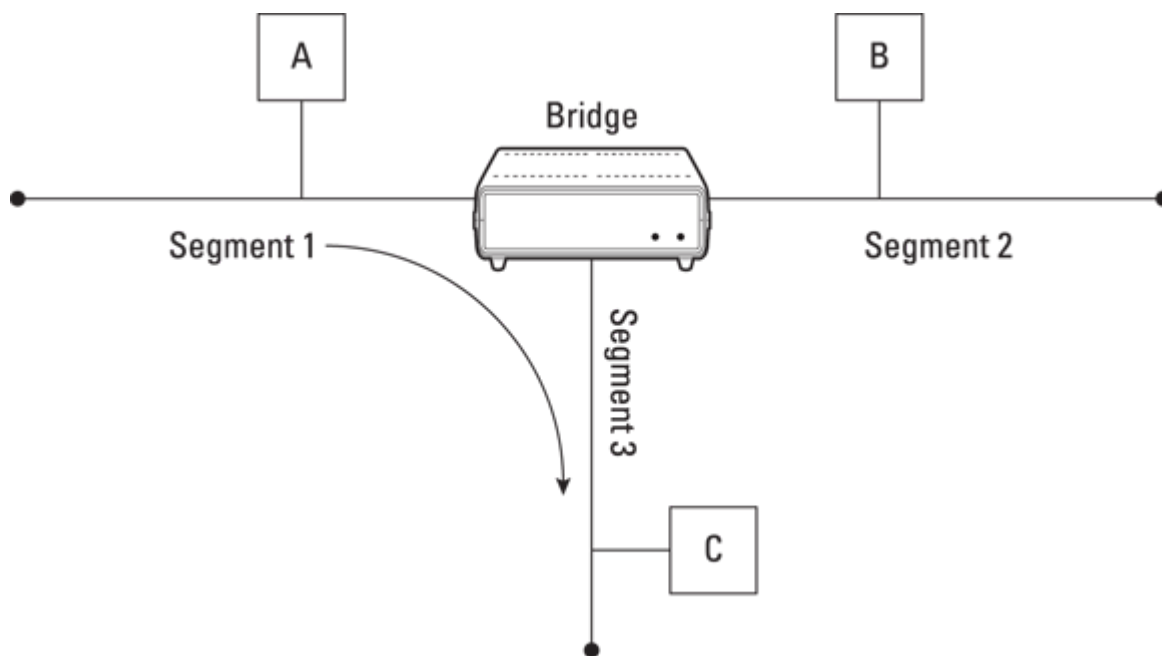


example, twisted pair cabling has a maximum length of 100 meters, so you need to ensure each cable length you are joining together with an extender does not exceed 100 meters.

## ***Bridge***

Because all data passing through a repeater is regenerated and sent to all parts of the network, a great deal of network traffic is generated that affects the overall performance of the network.

To prevent this buildup of network traffic, you can use a bridge (as shown in [Figure 1-20](#)), which is a device that connects network segments and also regenerates the signal (like a repeater). A bridge also filters the data so that it is sent only to the proper portion of the network, cutting down on network traffic and increasing overall performance.



**FIGURE 1-20:** A bridge forwards network traffic to only the destination segment.

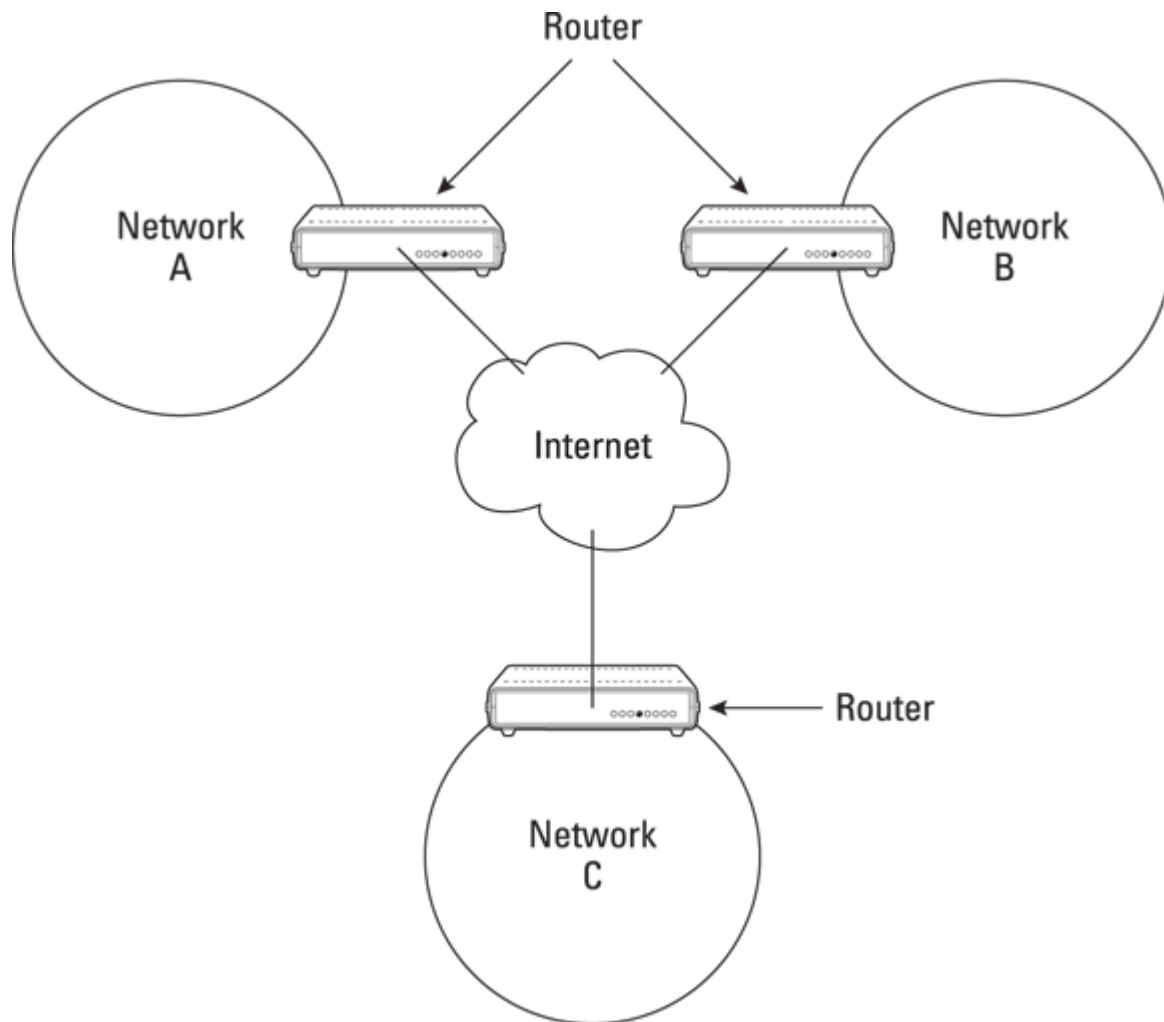
[Figure 1-20](#) illustrates that when computer A sends information to computer C, the information travels along segment 1 and eventually reaches the bridge. The bridge looks at its *bridging table* (a list of MAC addresses and corresponding network segments that runs in memory) to see which network segment computer C exists on. In this example, it lives on segment 3. At this point, the bridge forwards the information only to

segment 3, where computer C resides, and not to any other segment, thus filtering traffic and cutting down on network noise.

Bridges increase performance on the network by filtering the network traffic, which gives the network and all its devices and applications more bandwidth to work with. The less network traffic, the less chance of collision and retransmission.

## ***Router***

A *router*, which is responsible for sending information from one network to another, is an important network device because most companies are connected to the Internet. When a computer on your network wants to send information to a computer on another network, your computer passes the information to your router. [Figure 1-21](#) shows three different networks, each connected to the Internet by a separate router. All computers on network A know that any information with an outside-network destination must be passed to the router because the router is the only device with a physical connection to the outside world.



**FIGURE 1-21:** Routers send data from one network to another.

## *Gateway*

In theory, a *gateway* is a network device responsible for converting information from one format to another. Think of a gateway as a translator between two different languages: As information passes from one side to another, the gateway “translates” the information to a format that can be understood on the other side.

In today’s day and age, the gateway (or default gateway) is associated as the way off the network, which is the router.



FOR THE  
EXAM

You might encounter questions on the A+ exams in which you must identify the device based on a description. For the A+ exams, remember that a *gateway* is a device or piece of software that translates data from one format to another.

## Hub

A *hub* is a central device that acts as a connection point for all hosts on the network. A hub is a very basic device that passes all data that hits the hub to every port on the hub. This means that when a computer sends data to another computer, all systems will see the data on the network even though only the destination system for the data will process the data.

[Figure 1-22](#) shows a network hub.



**FIGURE 1-22:** A network hub with eight RJ-45 ports and one BNC port.

As the number of hosts on the network grows, you can “cascade” or connect one hub to another. Any data that reaches a port on a hub will be sent to all ports on all connected hubs, which could congest the network with traffic.



**REMEMBER** As I mention earlier, today's networks use switches instead of hubs. The term "hub" is used in this chapter only so that you know what a hub is in case you come across it in conversation or readings.

## Switch

A network *switch* is a device that looks similar to a network hub but differs in that the switch does not forward the data to all ports like a hub would. Instead, the switch filters network traffic by only sending the data to the port that the destination system resides on. [Figure 1-23](#) shows a network switch.



**FIGURE 1-23:** A 24-port network switch.

Switches can dramatically increase network performance because they filter the traffic by sending the data only to the destination port on the switch instead of to all ports on all hubs. Switches also offer security benefits because a system that is not the destination of the information does not receive a copy of the information, thus reducing the opportunity that someone other than the intended recipient can see your information.

Most switches today also offer security features such as port security, which enables you to limit which systems can connect to a port on the switch by MAC address. You can also control which ports a system can send data to!

When looking at switches you will notice that some switches are labeled "managed switches," while other switches are labeled "unmanaged." A

*managed switch* means the switch has an administrative interface for you to use that allows you to configure the switch and its features. Common features on managed switches include the ability to disable/enable ports on the switch, configure a port to only allow a specific MAC address to connect to it (known as port security), copy traffic and send to a specific port (known as port mirroring), and divide the ports into different LANs (known as VLANs).

An *unmanaged switch* does not give you an administrative interface or options to configure the switch. The unmanaged switch is just acting as a connection point for all the systems to communicate, with no fancy capabilities to customize how the switch operates.

### ***Wireless access point (WAP)***

A very popular network component today is a wireless access point. A WAP, typically connected to a wired network, is responsible for accepting data from wireless clients and then passing that data to systems on the wired network. The wireless access point can also receive information from the wired systems and then send that information to the wireless systems.

You can find a number of popular brands of wireless access points, such as Linksys, D-Link, and NetGear. Wireless access points that include additional features, such as firewall capabilities, are *wireless routers*.

[Figure 1-24](#) shows a wireless router used by home and small office networks.



**FIGURE 1-24:** A four-port wireless router also contains a WAN link for the Internet connection.

A wireless router has an antenna that collects the radio waves that carry the data from the wireless client. The wireless router also has a WAN port on it so that you can connect your Internet cable into it and share the Internet connection with all systems on the network. The WAP in [Figure 1-24](#) also has four additional RJ-45 ports to connect four wired systems.

The WAP is a multifunction device in the sense that it not only allows wireless clients to connect to the network, but it is also a four-port switch, allowing wired clients to connect to the network.



## *Patch panel*

When wiring your office to create a network, you will typically have network jacks in the wall to connect the workstations. Those network jacks will have a cable connected that runs through the wall to a wiring closet that contains a patch panel. The *patch panel* is the central device that all the wall jacks connect to. You then will connect the jacks of the patch panel to ports on a switch using a *patch cable*.

## *Other networking devices*

You may find a wealth of different network devices out there on different networks. Some other common network devices you may find are

- » **Modem:** The modem is used to dial-up across the phone line to another network and gives a remote user access to network resources.
- » **NAS:** Today's networks have network attached storage (NAS) devices, which are an enclosure that contains a number of hard drives that connect to the network.
- » **Firewall:** Most networks and systems today have firewalls that are used to limit the type of traffic that can enter the network or system.
- » **VoIP phones:** To carry voice over an IP network using voice over IP (VoIP), many companies today have VoIP phones that are connected to a network.
- » **Ethernet over power:** Ethernet over power involves connecting an Ethernet over a power adapter to the power outlet in the wall. You can then connect a workstation to the adapter that is plugged into the wall and use the power lines to carry network traffic. This is useful when you have an area of the building where you cannot run network cables; simply use the power lines to the outlets.
- » **Power over Ethernet (PoE):** Power over Ethernet is a way to carry power within the network cable along with the data. The benefit of this is that you can take a PoE device, such as an IP phone, IP camera, or wireless access point, and send power to it (using the network cable) without needing a separate power source for the phone. To leverage PoE, you must have a PoE-compatible network switch,



which is the source of the power, and a PoE-compatible device that receives the power from the switch over the network cable. If you have a non-compatible PoE network switch, you can purchase PoE injectors, which are devices that can act as a power source. These injectors are connected between the switch and the PoE device.

- » **Internet appliance:** A number of different Internet appliances can exist on the network. These appliances can act as proxy servers that filter what websites users can visit and cache web content.
- » **Cloud-based network controller:** A cloud-based network controller is a special network card that connects the router on your LAN to a software-defined network in the cloud.
- » **Cable/DSL modem:** A cable modem is a device that gives you high-speed Internet access from the cable company, which acts as an ISP. The cable modem will have an Internet line connect to it, and then it will connect to your home router to provide Internet access to the rest of the house or business. A DSL modem performs the same function but comes from the phone company. You can learn more about these devices in Book 8, [Chapter 2](#).

## *Understanding Communication Methods*

Different network devices, such as network cards, support different methods of communication. The three major communication methods in the computer world are simplex, half-duplex, and full-duplex:

- » **Simplex:** A device that supports simplex communication can deliver information in only one direction. Typically, the device can send information but cannot receive information.
- » **Half-duplex:** A device that supports half-duplex communication can deliver information in two directions, but not at the same time. A typical example of a half-duplex device is a walkie-talkie or CB radio, which enables you to send and receive information but not at

the same time. When you use a CB radio, you say “Over” to let the person on the other end know that you are done talking and that it is the other person’s turn to send information.

- » **Full-duplex:** A device that supports full-duplex communication is one that can send and receive information at the same time. Full-duplex is similar to talking on the phone: You are free to speak and to listen at the same time.

It is important to understand duplexing as you can experience networking problems due to duplexing mismatch. If your network card is configured for full duplex and the port on your network switch has been configured for half duplex, the system will not be able to communicate with the switch.

When purchasing networking or other types of devices for your computer, it is important to know whether you are buying a simplex, half-duplex, or full-duplex device to avoid problems later. For example, a musician friend of mine wanted to record his own material on the computer with recording software. After recording the first track, he had a problem recording a second track because his sound card was only a half-duplex device. He wanted to listen to the first track while playing along and recording the second track, which was impossible with his half-duplex sound card. He needed to have the sound card send and receive information at the same time, something that a half-duplex device can’t do. The solution: Get a new, full-duplex sound card.

## *Ways to Network a Computer*

If you want to build a small network with four computers in the home and have each system connect to the Internet, the best thing to do is to buy a home router from D-Link or Linksys. After you buy the home router, which is also a four-port switch, connect the four computers to the ports on the router and then plug the Internet connection into the WAN port. All systems are now interconnected and also to the Internet. But what if you need to connect two systems and you cannot connect them by using a hub or switch? You need to be aware of the different and varied methods used to network two computers, including the following:

- » Installing network cards
- » Using serial or parallel ports
- » Using infrared ports

The following sections describe the different computer networking methods.

### ***Network card***

The first task when using network cards to network two computers is to find out what type of network card you need for each system. You will have to find out whether the network card will be an PCI, PCIe, or PCI-X device. Open up the system and look at the different expansion slots that exist, or you can look at the documentation for the system.

After you purchase the network card and install it into your system, load the driver for the network card. If you're lucky and the network card is a Plug and Play device, the driver might load automatically for you, or you might be prompted by the OS to provide a manufacturer diskette with the driver for the device.

After you install the driver, you might have to spend some time troubleshooting the device because of resource conflicts with other existing devices. Once again, if you have a Plug and Play device, this step will probably not happen because the resources will be assigned dynamically by the OS.

### ***Serial and parallel ports***

You may also network two computers via the serial or parallel ports of both systems. Using standard parallel or serial ports for networking two devices can be a lot slower than networking two computers via a network card. You will connect the parallel ports with a *laplink cable*, and you will use a *null modem cable* for serial ports (RS-232 ports).

Here are the two networking methods that use serial ports:

- » Connect a modem to each computer's serial port and have the modems use the phone lines as the cabling.

- » Connect two computers directly by connecting the serial ports with a null modem cable.



**WARNING** If you try to connect two computers with a normal serial cable, the transmit data (TD) wire on one computer will be connected to the TD wire on the other computer, and the receive data (RD) wire on one computer will be connected to the RD wire on the other computer. No communication will occur in this situation. What you need is the TD wire on one computer connected to the RD wire on the other computer. A null modem cable is designed to do this, crossing the sending and receiving wires.

## *Infrared port*

Devices can also use infrared ports that can be used to connect to other devices on the network over short distances. For example, you can print to a printer sans parallel cable by using infrared technology.

*Infrared technology* uses an infrared light beam to carry data between devices. It typically requires clear line-of-sight — a clear path between the two devices. Infrared is limited in distance to about 100 feet and can transfer information up to 10 Mbps.



**ON THE  
WEB**

Lab 1-2 gives you some practice creating a small office or home network. Lab 1-2 can be found on the companion website at [www.dummies.com/go/aplusaio](http://www.dummies.com/go/aplusaio).

# *Troubleshooting Networking Issues*

Once the network is set up and systems are communicating, you will likely reach the day when communication is no longer working and the network is “broken.” In this section you learn about common network-

related issues with wired and wireless networks (keep in mind you will learn more about these topics as you progress through the next few chapters).

## ***Common wired and wireless network issues***

For the A+ exams you will be required to read a scenario and troubleshoot network issues based on the information in that scenario. The following are common symptoms related to wired and wireless network problems:

- » **Limited connectivity:** Limited connectivity is when you have some networking capabilities, but cannot access all network resources. For example, you may be able to access the LAN and not the Internet. This is common when there is no default gateway address assigned to the system, or the router connected to the Internet is not functional.
- » **Unavailable Internet resources:** If you are able to access resources on your network (called local resources), but not the Internet, there is typically a problem with the router. The router may be powered off, misconfigured, or maybe the connection to the ISP on the router is not working (meaning there is nothing wrong with the router and you have to call the ISP to find out what is going on with the ISP's connection).
- » **Unavailable local resources:** If you are unable to access resources on the network (called local resources), there could be a problem with your network card (if you cannot access any resources). If you can access some resources but not all, then the problem could be due to a misconfiguration on your network card such as the IP address configuration. The following are common local resources on your network you may have to troubleshoot access to:
  - *Shares:* Shares are folders published to the network from other systems like servers or workstations. If you are having trouble connecting to a share, be sure you have the share name correct, and the name of the system or IP address is correct that the share folder is running on. Once you have verified this information, verify that it is not a permission error, as you need to have permissions to shares in order to access them.

- *Printers:* If troubleshooting access to a printer, be sure you have the correct IP address for the printer, the correct printer driver installed, and that the printer is online and ready. Once you verify this, you then should check that you have permission to the printer as well.
- *Email:* If having trouble accessing email, verify that you have configured the email client software correctly with the correct server address and username and password.

There are a number of reasons why you may not be able to communicate with a wired or wireless network. The following are common problems I typically experience when troubleshooting networking:

- » **No connectivity:** You may experience no connectivity if an incorrect or corrupt network card driver exists on the system. When there is no network connection, re-install the network card driver and try replacing the network cable.
- » **APIPA/link local address:** Typically your system gets an IP address from the DHCP server when the system boots up. If the DHCP is not available to get an IP address, the system makes up its own IP address in the 169.254.x.y range. This could cause communication issues, as that is most likely not the IP range your network is using. In this case, you will need to verify the DHCP server is working. You learn more about IP addresses and DHCP in the remaining chapters in [Book 8](#).
- » **Intermittent connectivity:** When it comes to wireless communication, if you find you lose connections frequently, it could be because of interference from office/household items such as the microwave or a cordless phone. You learn more about this in [Book 8, Chapter 2](#).
- » **IP conflict:** If your system is trying to use an IP address that is already used on the network, you will get an IP conflict. In this case, you need to change the IP address on one of the systems.
- » **Slow transfer speeds:** If you find you are getting slow transfer speeds, you could check the speed setting on the network card and

verify that it is set to the correct speed. For example, using a 1 Gbps network card, I want to ensure the card is configured to operate at that speed. You can go into Device Manager and change the speed for the network card.

## *Using network troubleshooting tools*

One of the challenging parts of supporting networks today is knowing how to troubleshoot them. You find so many aspects of the network that it is difficult to know where to start your troubleshooting. The following is a listing of some common troubleshooting tools you should be familiar with for the A+ exams:

- » **Crimper:** A cable crimper is used to create network cables by attaching the connectors to the ends of the cable and then using the crimper to squeeze the connectors in place.
- » **Cable stripper:** A cable stripper is used to strip the outer layer off the cable so that you can get access to the wires.
- » **Multimeter:** A multimeter is used to test voltage and current and can be used to diagnose problems with a cable.
- » **Tone generator and probe:** A tone generator is used to locate cables in a mess of cables. You place the tone generator on one end of the cable and then place the toner probe on the other end of the cable to ensure that you have the right cable.
- » **Cable tester:** You can use a cable tester to verify connectivity from one end of the cable to another.
- » **Loopback plug:** A loopback plug is used to connect to a port and verifies that the port is actually working without sending data onto the network.
- » **Punch-down tool:** A punch-down tool is used by technicians to create the connections on a patch panel.
- » **WiFi analyzer:** A WiFi analyzer is a device that can monitor your wireless network environment and help identify potential issues. The WiFi analyzer can also identify the best channel to use for your

wireless network and identify the best location for your wireless access point on the network.

## *Getting an A+*

This chapter introduces you to a number of key concepts in network terminology. Understanding networking and how to troubleshoot the network has become an important skill for an IT professional, and you will be asked a few networking questions on the A+ exams. Remember the following points when preparing for the exams:

- » The three types of cables used on networks are twisted pair, coax, and fiber optic.
- » The three basic types of network layouts (topologies) are bus, star, and ring.
- » An access method determines how a system places data on the wire. Two popular access methods are CSMA/CD and token passing.
- » Ethernet is the most popular network architecture used today.
- » Some of the most popular networking devices are hubs, switches, and routers.
- » *Switches* filter network traffic by sending the data only to the port used by the destination system. *Routers* are responsible for sending data from one network to another.

## *Prep Test*

**1. What category of UTP cabling transmits data at 16 Mbps?**

- (A) Category 2
- (B) Category 3
- (C) Category 4
- (D) Category 5



**2. Which of the following defines simplex communication?**

- (A) Allows information to be sent and received, but not at the same time
- (B) Allows information only to be sent
- (C) Allows information to be sent and received at the same time
- (D) Allows information to be sent, but only after dependent information is received

**3. What is the transfer rate of Category 3 cabling?**

- (A) 2 Mbps
- (B) 10 Mbps
- (C) 16 Mbps
- (D) 100 Mbps

**4. Your manager has heard of being able to share a single public IP address through a feature called NAT. Which type of device should you install on the network to get NAT functionality?**

- (A) Switch
- (B) Hub
- (C) Repeater
- (D) Router

**5. What is the recommended number of users for a peer-to-peer network?**

- (A) Fewer than 100
- (B) More than 100
- (C) Fewer than 10
- (D) More than 10

**6. What access method is used for Ethernet?**

- (A) Token passing
- (B) CSMA/CA

- (C) Twisted pair
- (D) CSMA/CD

**7. Which of the following defines half-duplex communication?**

- (A) Allows information to be both sent and received, but not at the same time
- (B) Allows information only to be sent
- (C) Allows information to be sent and received at the same time
- (D) Allows information to be sent, but only after dependent information is received

**8. What category of UTP allows for data transfer at 1 Gbps?**

- (A) Category 3
- (B) Category 4
- (C) Category 5
- (D) Category 5e

**9. You would like to ensure that there is redundancy in connection points between systems. Which network topology should you use?**

- (A) Ring
- (B) Star
- (C) Bus
- (D) Mesh

**10. Which of the following best describes the functionality of a network switch?**

- (A) When data is received it forwards the data to all ports.
- (B) It translates information from one format to another.
- (C) When data is received it forwards the data to only the destination port.
- (D) It sends the data to the network of the destination system.

**11. Which of the following best describes a client-server environment?**

- (A) All users on the network connect to one another for the purpose of file sharing.
- (B) All users on the network connect to a central server and access resources on that central server.
- (C) All users on the network connect to one another for the purpose of printer sharing.
- (D) Each user accesses only one other user's computer.

**12. What is the maximum distance of UTP cable?**

- (A) 100 meters
- (B) 185 meters
- (C) 250 meters
- (D) 500 meters

**13. You are the network technician for your company. You are troubleshooting Bob's network connection and need to trace the network cable from Bob's workstation to the wiring closet. What tool should you use?**

- (A) Packet sniffer
- (B) Toner probe
- (C) Cable tester
- (D) Loopback plug

**14. You are looking to install a network cable that needs to travel through areas that have large machinery, which typically can cause electromagnetic interference. Which of the following cable types are less likely to be affected by interference?**

- (A) Fiber optic
- (B) 100BaseT
- (C) 1000BaseT

(D) Coaxial

**15. You have just purchased a DSL high-speed Internet connection for your home office. Which type of connector is used to connect the DSL router to the wall jack?**

(A) SC

(B) RJ-45

(C) RJ-11

(D) BNC

**16. Which of the following best describes full duplex communication?**

(A) Allows information to be both sent and received, but not at the same time

(B) Allows information only to be sent

(C) Allows information to be sent and received at the same time

(D) Allows information to be sent, but only after dependent information is received

**17. What Ethernet architecture transfers information at 1 Gbps over short distances and uses fiber optic cabling?**

(A) 1000BaseSX

(B) 1000BaseLX

(C) 1000BaseTX

(D) 100BaseTX

**18. You are the network technician for the office and have decided to create some CAT 5e cables to connect workstations to the network. What type of connector do you crimp onto the ends of a Category 5e cable?**

(A) SC

(B) RJ-45

(C) RJ-11

(D) BNC

**19. What is the maximum distance of fiber optic cabling?**

- (A) 100 meters
- (B) 185 meters
- (C) 500 meters
- (D) 2 kilometers

**20. Your manager decided that the company should look at using fiber optic cabling, but is concerned about purchasing the correct network cards. Which of the following represents a connector used by fiber optic cables?**

- (A) BNC
- (B) RJ-45
- (C) RJ-11
- (D) LC

## *Answers*

1. **C.** Category 4 UTP cabling transfers data at 16 Mbps. See “[\*Twisted pair.\*](#)”
2. **B.** Simplex devices deliver information in only one direction. Review “[\*Understanding Communication Methods.\*](#)”
3. **B.** Category 3 cabling transfers information at 10 Mbps. Check out “[\*Twisted pair.\*](#)”
4. **D.** A router is a device that provides NAT functionality. Peruse “*Router.*”
5. **C.** The recommended number of computers in a peer-to-peer network is ten or fewer. Take a look at “[\*Peer-to-peer networks.\*](#)”
6. **D.** CSMA/CD is the access method that is used in all Ethernet environments. Token passing is used in token ring architectures, and

CSMA/CA has been used in AppleTalk networks. *Peek at [“Ethernet.”](#)*

7. **A.** Half-duplex devices allow you to send and receive information, but not at the same time. *Look over [“Understanding Communication Methods.”](#)*
8. **D.** Category 5e UTP cabling transfers data at 1 Gbps. *Study [“Twisted pair.”](#)*
9. **D.** In a mesh topology, each device is connected to each other device, which means that a system can use different pathways (redundancy) to contact any other system. *Refer to [“Mesh.”](#)*
10. **C.** When a switch receives traffic it looks to its MAC address table to determine on what port on the switch the destination system resides. It then forwards the traffic to only that port. *Examine [“Switch.”](#)*
11. **B.** Client-server environments are implemented for the purpose of centralized administration and security. It is much easier for an administrator to control resources if he is sitting at one computer and all users connect to that one computer. *See [“Server-based \(client-server\) networks.”](#)*
12. **A.** The maximum distance of UTP cable is 100 meters. *Review [“Twisted pair.”](#)*
13. **B.** Tone generators and toner probes are used together to help locate a specific cable in a batch of cables. You place the tone generator on one end of the cable, and then place the toner probe on the other end of the cable to see if you can pick up on the tone from the tone generator to identify the cable. *Check out [“Using network troubleshooting tools.”](#)*
14. **A.** Fiber optic cables send information in pulses of light through a glass core. Because the signal is not an electrical signal, it is not susceptible to electromagnetic interference. *Peruse [“Fiber optic.”](#)*
15. **C.** DSL Internet connections are provided by the phone company. As a result, they use the same connector type as the phone. *Take a look at [“Twisted pair.”](#)*

16. **C.** Full-duplex devices can send and receive information at the same time. *Peek at “[Understanding Communication Methods](#).”*
17. **D.** The 1000BaseSX Ethernet architecture can transfer information at 1 Gbps over fiber optic cabling using short distances. *Look over “[Gigabit Ethernet standards](#).”*
18. **B.** RJ-45 connectors are the connectors used by twisted pair cabling. *Study “[Twisted pair](#).”*
19. **D.** Fiber optic cabling has a maximum distance of about 2 km. *Refer to “[Fiber optic](#).”*
20. **D.** The LC connector is a connector type used by fiber optic cabling. *Examine “[Fiber optic](#).”*

## Chapter 2

# Understanding Common Wireless Communications

---

### IN THIS CHAPTER

- » Identifying infrared, Bluetooth, cellular networks, and 802.11 wireless network characteristics
  - » Optimizing features of 802.11 wireless networks
  - » Identifying security settings for 802.11 access points and wireless networks
  - » Installing and configuring a SOHO network
  - » Connecting to 802.11 wireless networks
- 

Once the domain of cutting-edge techno-geeks, wireless technology is now for everyone. Wireless technology has entered all aspects of our lives, so as a CompTIA A+ Certified Professional, you need to deal with wireless connectivity. This chapter gives you an overview of the technologies involved.

The main types of wireless devices that you see in this chapter are infrared, Bluetooth, cellular networking, and 802.11 wireless networking.

## *Understanding Infrared Devices*

Of the wireless technologies I cover in this chapter, infrared is the technology that has been around the longest and is likely the most stable in its development. *Infrared* uses light beams in the infrared spectrum, which is beyond the visible light spectrum. You likely use infrared technology daily if you use a remote control for your TV or DVD player. This technology, when used with computerized equipment, follows the



standards of IrDA (Infrared Data Association). You can find more information about the association and infrared standards at

[www.irda.org](http://www.irda.org).

Infrared is a *line-of-sight* technology; it requires a direct, unobstructed view between the transmitter and the receiver. Because infrared is line-of-sight, it has obvious limitations as to where it can be used. Any objects obstructing the line of sight prevent data transmissions. (Nothing more frustrating than trying to change the TV channel with someone blocking the set.) However, the benefit of line-of-sight is that you do not have interference from or interference with areas outside the line-of-sight, such as devices in the next room.

The goal of infrared networking was for short range (less than a meter), direct line-of-sight ( $\pm 15^\circ$  cone), and low speed (technologies between 1.6 Kbps and 2.4 Kbps). There are many different specifications, each with a different speed specification. One of those specifications is used for open office–networking, a technology that has been replaced by 802.11b and involved infrared repeaters placed around an office.



FOR THE  
EXAM

Most tasks handled by infrared technology have switched to use newer 802.11 networks and Bluetooth technologies, which use radio frequencies (RF).

## *Working with Wireless Networks*

“Why do I need a wireless network?” was a question people used to regularly ask. You will not hear this question much anymore, though. The main reasons why people want wireless networks these days are increased mobility and to avoid cabling issues.

When wireless networks started, they had access speeds of 1–2 Mbps; current standards have network speeds higher than 100 Mbps. At one time, wireless networking equipment was a premium addition to a

network, but this equipment has become a commodity and is inexpensive enough that anybody can start up a wireless network.



**WARNING** Wireless networking should not be used for a primary network because of its limitations, such as obstructions and interference. (See “[Troubleshooting Issues](#),” later in this chapter.) If the user knows what those limitations are, the network should be considered a best-effort network — and as such, it should not be expected to be available or to function at full speed at all times. As a secondary network, though, wireless networking does offer a great deal of flexibility for getting to your data. Any devices that exist on your normal wired network can be present on your wireless network, including firewalls, servers, and printers.

## *Components of a wireless network*

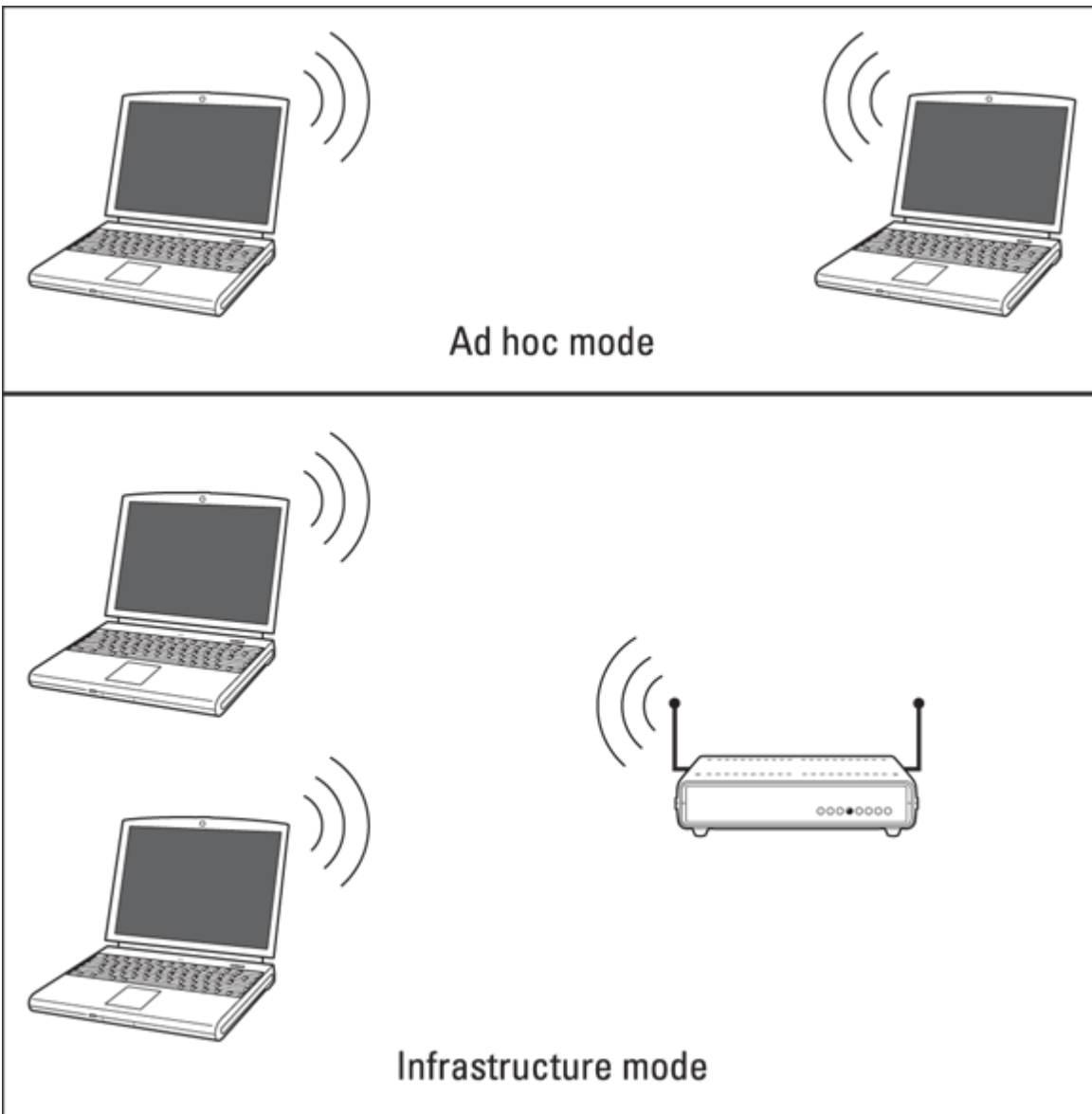
The two main components of wireless networks are clients and access points. *Clients* are computers with wireless network cards; these cards work just the same as wired network cards, but without the wires. *Access points*, which act as a consolidation point for multiple wireless clients, have a connection to a traditional wired network. Some new access points allow linking multiple access points through wireless links, extending the range and coverage of a wireless network without having all access points connected to a wired network, thereby saving on wiring costs.

Most laptops now include wireless network cards as an integrated feature, and wireless network cards are available for desktop computers, connecting through PCI, PCI Express (PCIe), or USB. It is great that many computers have integrated wireless cards, but be prepared as new technology arrives on the scene since you will likely end up using an expansion option on your computer to add an updated wireless card to your computer.

Wireless networks used to command a premium, but wireless networking components have become a commodity. You now have several choices, all less than \$100. The difference in price between the inexpensive units

and expensive units is based on the strength of the radios, the features that are available on the unit, and the brand.

If you work with a wireless network that has an access point, the network client runs in *infrastructure mode*, which has access points making up the underlying network infrastructure. If the network is composed only of clients joined to form a network, the network runs in *ad hoc mode*, which is typically used only when people need to exchange files or work together in a location without an access point. This type of work situation often happens when people use a temporary location — say, a conference room — to work on a project for a couple of days. Instead of relying on a 4–8-port mini-switch or hub with which files could be shared, folks can just use an ad hoc wireless network. Both wireless network types are shown in [Figure 2-1](#).



**FIGURE 2-1:** Wireless networks are usually run in infrastructure mode but can also be run in ad hoc mode.



**FOR THE  
EXAM**

Most wireless networks are composed of access points and wireless clients, so unless the question specifies *ad hoc*, access points should be expected to be on the network.

## *Connecting to a network*

Every wireless network is identified by an SSID (Service Set Identifier), which is used by all clients on the network, identifying them as members of the network. The *SSID* is a case-sensitive name of 32 or fewer characters. Every manufacturer sets a default SSID. However, for security and to reduce confusion with neighboring access points, this default should be changed to a unique name. To connect to a wireless network, you need to know the SSID.



TECHNICAL  
STUFF

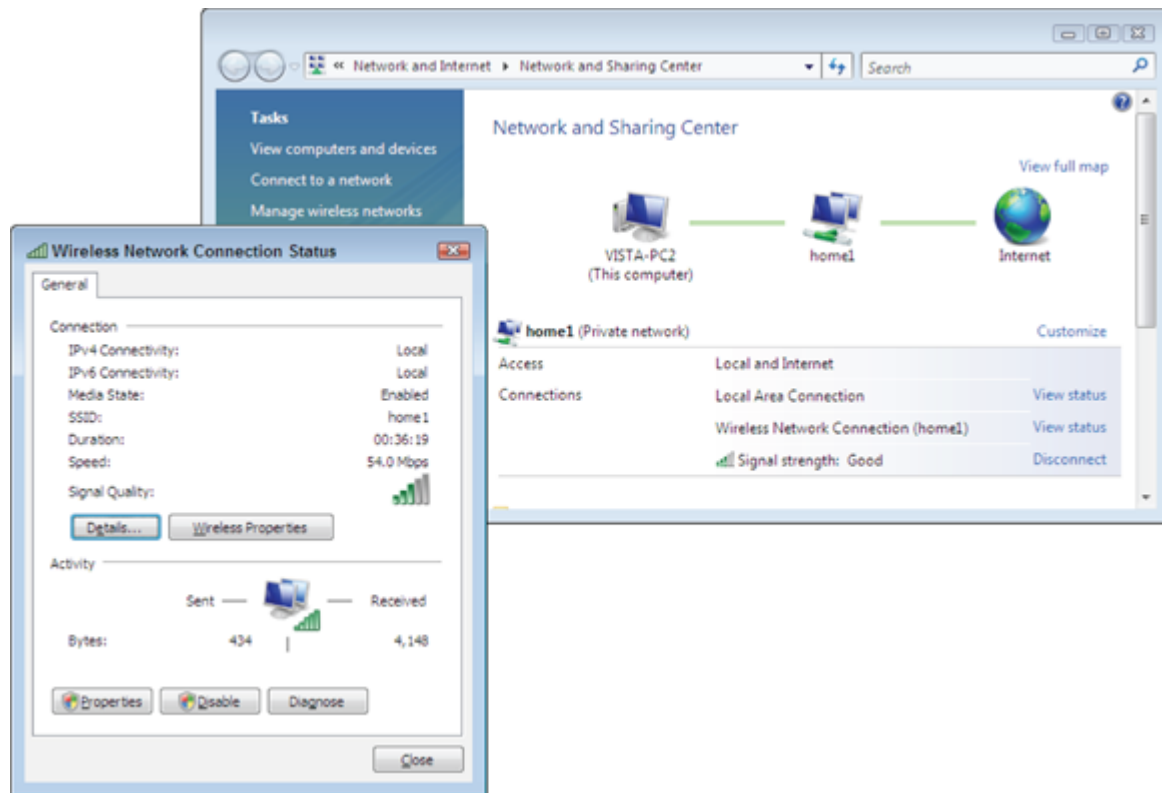
Some manufacturers refer to the SSID as a BSSID (Basic Service Set Identifier) or an ESSID (Extended Service Set Identifier). The IEEE 802.11-1999 wireless network standard defines an ESSID as a set of access points using the same SSID and channel, and operating as a single BSSID to their wireless network clients.

After your wireless network card driver is installed you can then connect to the wireless network by its SSID.

### ***Windows 7, Vista, and Windows 8.1***

If you use the default Windows 7, Vista, and 8.1 software, open the Network and Sharing Center and click the View Status link next to your wireless card. This provides you with information such as connection speed, SSID, and signal strength. If you are not yet connected to the network, click the Manage Wireless Connections link in the Network and Sharing Center. From there, you can choose to add a new wireless network manually or by viewing from the networks in your area that are broadcasting their SSIDs.

To configure a connection to one of the networks, simply select the network and then click the Connect button. When connecting to a wireless network, if you need to enter a security key, you are prompted to enter the required information. Both the Network and Sharing Center and the Wireless Network Connection Status dialog box are shown in [Figure 2-2](#).



**FIGURE 2-2:** Windows wireless settings are accessed via the Network and Sharing Center.

## *Windows 10*

You can use the same process to manage networks in Windows 10 by going to the Start menu, typing **control**, and choosing Control Panel from the Best Match section of the Start Menu. Once in the Control Panel, choose Network and Internet ⇒ Network and Sharing. You can also see a list of wireless networks by clicking the wireless icon in the notification area of the taskbar. If you click on a wireless network, you are presented with a Connect button that allows you to connect to that network. Once connected, you can choose the Properties link to view the settings of that network.

## *Wireless standards and protocols*

Wireless networks are defined by several standards, and the performance and security features for wireless networks are constantly improving. What's more, because of constant improvements, new standards continually emerge. Gordon Moore of Intel predicted that the components in a processor's integrated circuit would double every 24 months. This

statement has since been named Moore's Law, and has been applied to many areas of the computing industry. As Moore's Law is applied to more sections of the computer industry, wireless is just another section of the industry that falls to those general rules, with speed doubling every two years.

The main wireless standards currently in use are 802.11a, 802.11b, 802.11g, and 802.11n, with other standards on the horizon. Each of these technologies is based upon published standards, and the upcoming ones are usually based upon several draft standards. Some hardware manufacturers have started to supply hardware capable of supporting the upcoming standards and using some of the new features. Typically, if the manufacturer can meet the hardware standards, the software can be updated later via a firmware update.

To go along with the standard features, many vendors choose to implement additional features not in the standard or make propriety enhancements, like many of the vendors who advertise special speed enhancements.

The following sections outline the main features of each of the 802.11 wireless networking standards.

### ***802.11a***

Released in 1999 (but not actively shipping until component supply issues were resolved), 802.11a networks operate in the 5 GHz radio spectrum. Other devices, such as newer cordless phones, also run in this unlicensed spectrum. Overall, the 5 GHz space is less occupied by devices compared with the 2.4 GHz space used by most other wireless devices. For 802.11a networks, there are 12 non-overlapping signal channels.

The network rated speed of 802.11a is 54 Mbps, but in most situations you can expect to see about half that speed. The typical range for this type of network is about 100 feet (30 meters).

Although the 5 GHz frequency range is unlicensed, its use for wireless networking has been approved only in the United States, Canada, and Japan; and prior to 2002, only in some European countries. Regulatory

changes in 2002 and 2003 opened the 5 GHz frequency range throughout the European Union.

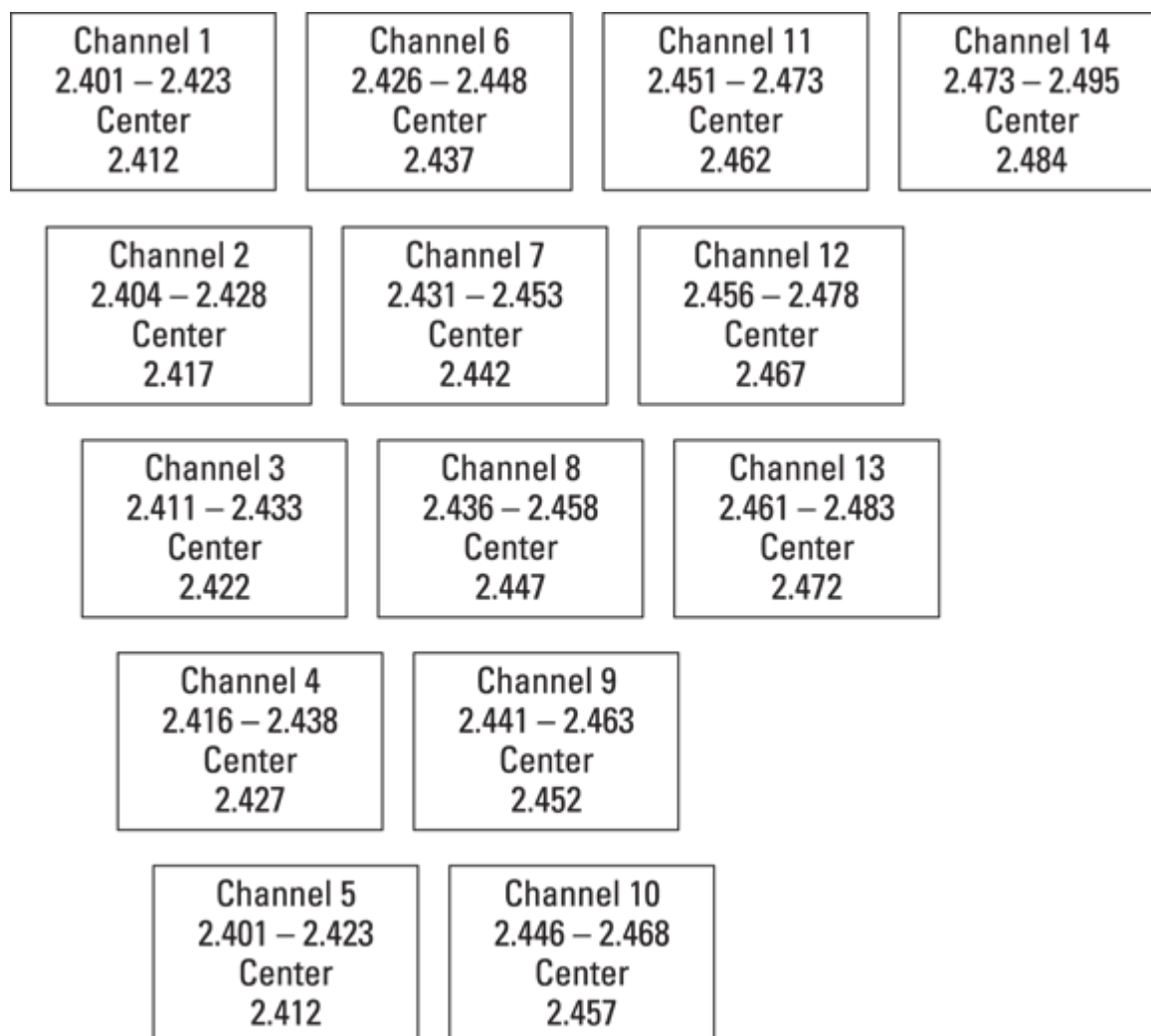
### ***802.11b***

Released in 1999, 802.11b technology was able to beat 802.11a technology to the market because it was built on DSSS (Direct-Sequence Spread Spectrum) technology. As such, components required for it were all readily available for production facilities. 802.11b operates in the 2.4 GHz radio spectrum, which is heavily cluttered with cordless phones, Bluetooth (see the “[Bluetooth](#)” section, later in this chapter), and spill-over interference from microwave ovens.

The network rated speed of 802.11b is 11 Mbps, but in most situations you can expect to see about 6.5 Mbps because 802.11b is a CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) network, which sends “I’m going to send data” broadcast messages prior to sending its data, which increases the traffic on the network. (See Book 8, [Chapter 1](#) for the lowdown on CSMA/CA.) The typical range for this type of network is about 100 feet (30 meters).

Wireless networks in the 2.4 GHz range have 14 channels available for use. Eleven channels are acceptable everywhere, the United Kingdom and some European countries allow up to 13 channels, and Japan allows all 14 channels. Channels are defined by the center frequency that they use. Some vendors use wider channels than others, overlapping their neighboring channels. Typically channels 1, 6, 11, and 14 are thought to be non-overlapping, so in North America there are three channels that are normally non-overlapping and will not interfere with each other. See [Figure 2-3](#) for a channel diagram of the 802.11b/g spectrum. The point here is if you are experiencing intermittent problems with a wireless system, try changing the channel on the wireless router to either 1, 6, or 11, as you could be experience problems due to interference with other wireless devices running on the same channel.





**FIGURE 2-3:** Normal channel frequencies used for 802.11b/g networks.



**FOR THE  
EXAM**

Remember for the exam that channels 1, 6, and 11 are considered non-overlapping channels. If your wireless environment is experiencing intermittent connection issues, it could be due to interference with other wireless networks, a microwave, or a cordless phone, for example. As a fix, you can experiment with changing the channel on your wireless access point to one of the non-overlapping channels.

**802.11g**

Released in 2003, 802.11g is an updated version of 802.11b, still running in the 2.4 GHz spectrum but allowing faster data transfer speeds to put it on a performance par with 802.11a. Because it operates in the 2.4 GHz spectrum, it is also backward compatible with 802.11b, making migration to 802.11g an easy step for many organizations because they could update the back-end infrastructure and then update the wireless clients in a manner that fits within the corporate requirements.

The network rated speed for 802.11g is 54 Mbps, but in most situations you can expect about half that speed because the throughput is reduced as distances between the client and access point increase, and the signal suffers from greater interference. Because wireless networks are a shared medium further reduces throughput as the number of users sharing an access point increases the competition for the wireless signal. The typical range for this type of network is about 100 feet (30 meters).

With all the benefits that are available with 802.11g, many companies began producing products well before the standards were ratified.

### ***802.11n***

802.11n represents the latest improvements to networking in the 2.4 GHz and 5 GHz spectrums. Originally planned as a replacement for 802.11b/g, the standard now allows for radios operating in the 5 GHz spectrum of 802.11a. Again, this solution suffers from an already congested spectrum. The biggest change that you will see with this technology is the implementation of multiple transmitters and receivers and multiplexing of signals. This technology is referred to as MIMO (Multiple-Input Multiple-Output).

The network-rated speed is up to 200 Mbps (600 Mbps when multiplexed or connected over multiple radios). As with most wireless technology, you should expect typical transfer rates at about half that — in the 300 Mbps area. The typical range for this type of network is about 165 feet (50 meters).

### ***802.11ac***

The newest of wireless standards is the 802.11ac wireless standard, which uses the 2.4 GHz or 5 GHz frequency range. The 802.11ac wireless

standard has different transfer rates depending on the implementation, but expect them to be faster than 802.11n. Transfer rates could be from around 500 Mbps to gigabits per second depending on the number of antennas and configuration of the access point. For example, a two-antenna access point could reach speeds of 867 Mbps, while a three-antenna access point could reach speeds of 1.27 Gbps.

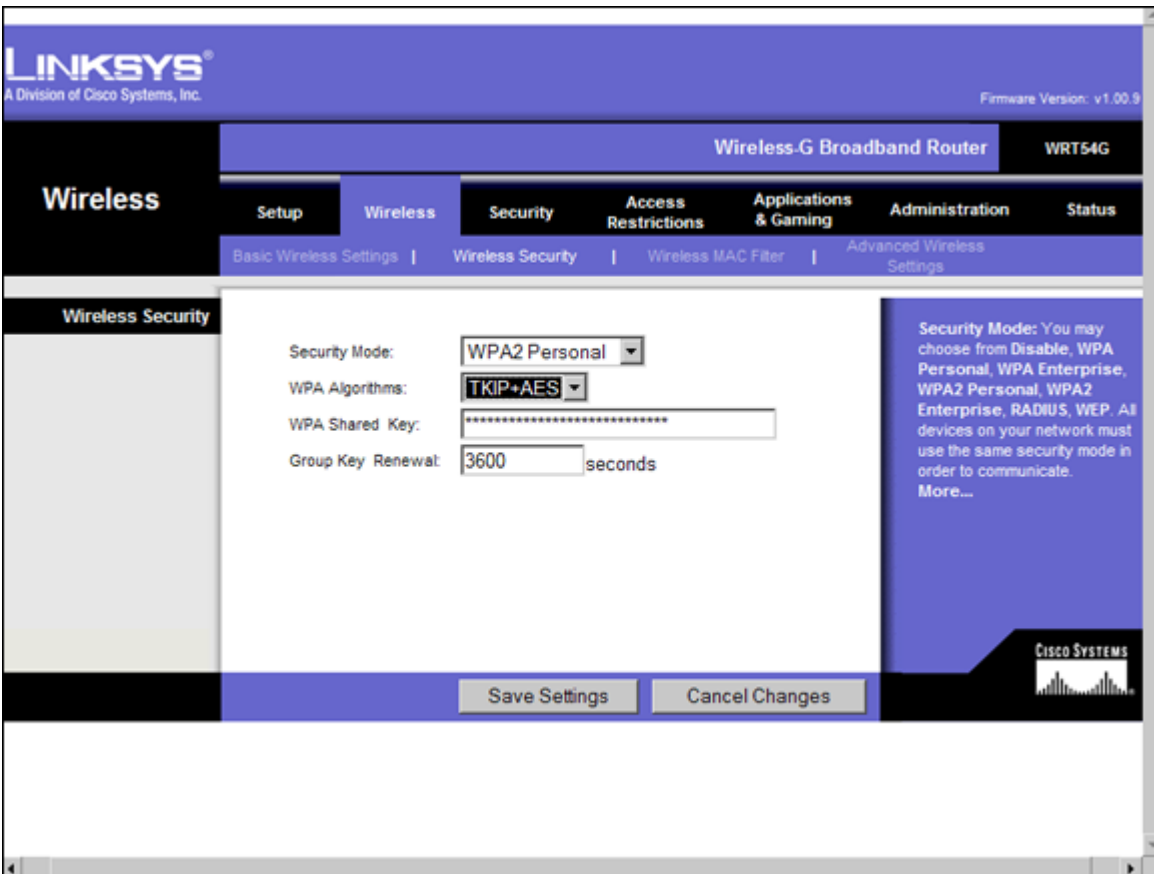


TECHNICAL  
STUFF

Although there is a lot of talk about cordless phones causing interference with wireless networking, there has been a big boost in 6 GHz phone sales because they do not interfere with 802.11b/g/n/ac networks.

## *Securing wireless networks*

With the proliferation of wireless technology, security has come to the forefront of many conversations, which is odd because it should have been prominent from the very beginning. The main steps you can take to improve wireless security include password management, SSID management, MAC address filtering, WEP, WPA, WPA2, DMZ, DHCP settings, and updating the firmware. Many of these configuration settings can be seen in [Figure 2-4](#). The configuration screens for most access points are accessed using a web browser and connecting to the IP (Internet protocol) address of the access point, as I did when connecting to the Linksys access point shown in [Figure 2-4](#).



**FIGURE 2-4:** Security options for a typical wireless access point.



**WARNING** It is important to note that although I discuss common security options for wireless networks, most security methods are easily bypassed by a determined hacker. WEP and WPA are fairly easy encryption methods to crack and MAC filtering is fairly easy to bypass. For the A+ exams you need to know steps to take to secure wireless, but know in the real world that you should implement many security measures.

### ***Passwords***

All access points ship with a default Administrator username and password. A quick search of the Internet will give you the default usernames and passwords for most manufacturers and models. Usually, in addition to an owner's manual, a new access point will ship with a Quick

Start guide containing an abridged set of steps to follow to apply a basic configuration to the access point. This guide typically includes the default IP address, username, and password used by the access point. When wireless networks started to become widespread, these guides did not suggest changing the default passwords, but most of them now offer the suggestion in the initial setup steps — if not actually forcing you to do it before making any other configuration changes.



**REMEMBER** Changing the Administrator password should be the first step in the setup procedure. Until you change the password, any people within the range of your access point can make any configuration changes they wish.

### ***SSID broadcasting***

Security through obscurity is not the best security measure, but it provides one more layer to your overall network security. Most operating systems such as Windows, Linux, and MAC OS, try to make it easy for you to connect to wireless networks by displaying the SSIDs for wireless networks in range of your computer if the access points are broadcasting their SSID. This allows you to select the SSID or wireless network that you want to connect to and quickly configure it. By disabling the broadcasting of your SSID, your network will not show up in the list of detected wireless networks within Windows or other operating systems. If you are not on the list, most people won't even know your network is there — and therefore, won't connect to it. Windows 7 will display nonbroadcasting SSIDs as wireless networks named "Other Network." Connecting to the "Other Network" will require the user to know the actual SSID.



**WARNING** Disabling SSID broadcasting is only a mild security setting, as you discover in the section, "[Troubleshooting Issues](#)," later in this chapter. If someone wants to gain access to your wireless network,

disabling SSID broadcasts won't slow him very much nor prevent that person from knowing that a wireless network exists.

### *MAC address filtering*

Media Access Control (MAC) address filtering is another step that will slow most casual users from gaining access to your network, but it is not considered strong security on its own. Most access points allow you to perform different types of filtering, and most allow you to at least filter traffic by MAC addresses that are hard-coded onto each network adapter on your wireless network.

Implementing this security step means that for each new network card that you want to operate on your network, you need to adjust your access points. Even with the MAC address restriction in place on your access point, an unscrupulous person can use a network sniffer like AirSnort to see some traffic on the wireless network. In this traffic, such a person can see the MAC addresses of clients who are communicating on your wireless network. By taking this information and using a network card or operating system that allows him to manually control the MAC address, the individual can imitate one of the valid MAC addresses that are allowed to be used on your network. The timing on this is important because if two computers on a network have the same MAC address, all sorts of communication errors can happen.



**WARNING** As I mention previously, MAC address filtering keeps the casual user out of your network, but it shouldn't be your sole security measure. If somebody wants to get onto your network, this will not slow him down very much.

### *WEP*

The security measures I've discussed thus far do not deal with encryption. Wired Equivalent Privacy (WEP) was the first attempt to secure wireless networks by using encryption. Early WEP used a 64-bit key, which was a 40-bit encryption key joined with a 24-bit initialization vector (IV). This

was easily breakable. Newer WEP uses a 104-bit encryption key joined with the 24-bit IV, providing a higher level of security.

WEP was fairly easy to configure on both the access point and the client and again provides security against the casual wireless user. One of the main drawbacks to WEP is that technology has not substantially changed on how security keys are managed, such as IVs being sent over the network in plain text. And, if an intruder captures enough traffic from your network, he can deduce your WEP keys, giving him full access to your network. The answer to this problem is WPA.

## ***WPA***

WiFi Protected Access (WPA) and WPA2 (also called 802.11i) are all about improving security on wireless networks. Rather than using a single WEP key, WPA uses per-session keys that are agreed upon by the wireless client and the access point after an initial handshaking process. This technology was created in response to the weaknesses that were found in WEP. No security is unbreakable, and creating a better mousetrap just seems to create smarter mice. Still, the security settings available in WPA2 make wireless networks as secure as they can be. As of this writing, the time needed to break the keys used would render the broken keys mostly useless because they would have already been changed on the network.

You can implement WPA in one of two modes:

- » **WPA Enterprise:** With WPA enterprise when a client connects to the wireless network they are sent to a RADIUS server to authenticate before they can gain access to the wireless network. Authentication is typically done via a username and password which increases the level security over a simple wireless key.
- » **WPA Personal:** Is the mode you use at home, which involves setting up a pre-shared key on your router. Anyone wanting to connect must use that same pre-shared key in order to connect.

In your list of security methods, you can choose TKIP (Temporal Key Integrity Protocol), which uses a 128-bit encryption key and a 48-bit IV to

secure the data. In addition, after every 10,000 packets of data have been sent, new TKIP keys are generated and used. This regular changing of the keys keeps the network more secure.

## **WPA2**

WPA2 builds upon the security of WPA and operates in either Enterprise mode or Personal mode like WPA does. WPA2 improves the encryption by rotating keys, but also by using a more advanced encryption algorithm known as Advanced Encryption Standard (AES). AES allows for encryption keys of 128, 192, or 256 bits.



FOR THE  
EXAM

WPA2 encryption is the most common security method used to secure wireless networks because the data is encrypted with the password you use (known as the key), and the password acts as a method of authorizing the client (only systems that know the password can connect).

## **VPNs and DMZs**

Although it requires more setup, you can treat your wireless network as a hostile remote network. By *hostile*, I mean that the network contains many individuals who would like to gain access to the company's private information stored on its corporate network. Some companies have faith that the security settings that they configured on their wireless access points will keep all unwanted visitors or trespassers off their network. And that is not an unreasonable thought, given the current security settings that are available. However, for those companies that do not trust these security levels available in the current wireless technology, or who are afraid of the smarter mouse arriving on the scene sooner rather than later, other steps can be taken to provide even more secure wireless.

Most companies today have a connection to the Internet coming into their organization, and they treat the Internet as a large hostile remote network. To prevent their private data from being accessed, companies use a firewall where the Internet meets their network, allowing them to inspect



and control the data that moves between their network and the Internet. If they have data that they would like some people on the Internet to be able to access (such as data on a web server or an FTP server), they may implement a second firewall, making another private network. This strategy provides some protection from unwanted visitors gaining access to the web or FTP server but offers less protection than their normal private network because some people have a right to access the server. In most cases, this more open private net will be placed between the hostile Internet and the private corporate network, creating a less hostile, but still not absolutely safe, Demilitarized Zone (DMZ).

It is also common for companies to have remote workers who need access to the corporate network while they are away from the office. This access is given through a special secure channel: a Virtual Private Network (VPN). A VPN relies upon secure authentication and data encryption methods to create a secure and private connection through a firewall to a corporate network. Most often, this security is handled by SSL (Secure Sockets Layer) or IPSec (IP Security), which are two industry standard methods of encrypting TCP/IP or Internet data.



**TIP**

More information about firewalls, VPNs, DMZs, SSL, and IPSec can be found in Book 9, [Chapters 1](#) and [2](#).

So, by segregating your wireless users into their own DMZ or private segment (protected from the Internet), you can keep any potential wireless intruder away from your private corporate data because users of that wireless network do not have direct access to the corporate network. For your users to access corporate data, they use the same remote access methods, such as a VPN connection, that they would use when on the road. These additional security steps can be layered atop the previously discussed techniques, such as using WPA2 encryption, forcing users to take more steps to get access to your corporate data, but making the connection more secure.

### ***DHCP server settings***

A *DHCP* (Dynamic Host Configuration Protocol) server provides automatic TCP/IP configuration to network clients by changing normal items that DHCP provides, such as a default gateway or DNS settings for name resolution, or by disabling DHCP altogether. By failing to distribute accurate TCP/IP information to unwanted visitors, and using manual TCP/IP configurations to users, you are implementing another rudimentary security step. This security based on DHCP settings might prevent most casual users from getting ready access to information or gaining access to the Internet through your wireless network. Still, any unwanted intruder who wants to gain access will be able to find correct TCP/IP settings by using a standard packet capture utility, such as Wireshark ([www.wireshark.org](http://www.wireshark.org)).

### *Client isolation*

This option, available on many network switches, has found its way to wireless networks as well. When this setting is enabled, wireless clients can talk to the rest of the network but cannot communicate with other clients on the same wireless access point.

### *Firmware*

Not to be forgotten when setting up new wireless networks (or periodically after a network is set up) is to check for firmware updates for your wireless network components or driver updates for your network cards. These updates are how new security features are retrofitted into your wireless products.



**REMEMBER** Take care when doing this because features are occasionally removed, or you might encounter problems with the new code in the firmware.



**TECHNICAL STUFF** Many people have opted to stop using the firmware from their hardware manufacturer and instead use a third-party or open source

firmware, such as DD-WRT ([www.dd-wrt.com](http://www.dd-wrt.com)). This firmware works on a variety of hardware platforms, which are listed on its website.

### *Authentication with wireless*

In environments where security is a concern, you want to use more than just a passphrase to control who can connect to your wireless network. *Authentication* means individuals must identify themselves to the system and then verify they are authorized before they are granted access. There are different forms of authentication that can be used with wireless:

- » **Single-factor:** Single-factor authentication involves only a single piece of information being used to authenticate to the system. This could be a passphrase, such as the wireless key, or a smart card. Single-factor authentication could also use biometrics such as a retina scan or fingerprint scan.
- » **Multifactor:** Single-factor authentication systems are common, but not considered very secure. For example, most home wireless networks use a passphrase to connect to the wireless network (which is single-factor authentication — a single piece of information). The problem is, if someone learns this passphrase without you knowing, he now can connect to the wireless network. Multifactor authentication means that multiple pieces of information are used to authenticate to the system. For example, you must supply the smart card and know the PIN associated with that smart card.
- » **RADIUS:** RADIUS is a central authentication service that can exist on the network to implement authentication across different technologies. For example, you can build a RADIUS server that has a list of usernames and passwords and then configure your wireless access point to use that RADIUS server. This means someone would need to know a username and password in order to connect to wireless, not just a passphrase. That same RADIUS server can be used to authenticate folks connecting to the physical network by having the switch configured to use the RADIUS server. You can also

use RADIUS for authenticating VPN clients for remote access to the network from across the Internet.

- » **TACACS:** TACACS is a centralized authentication system used with Unix systems. TACACS+ is used by Cisco systems. The overall roll of the technology is the same — a central authentication system, but used with different products.

## *Installing and Configuring a SOHO Network*

The new A+ exams not only want you to understand the theory of wireless networking, but they also want you to have a basic understanding on how to set up a small office/home office (SOHO) network. In the following sections, you see some of the basic settings that need to be configured on a wireless home router. These settings may look different on each different model of wireless router, but the concepts are all the same.

I am using a DLINK DIR-615 router as the example.

When you take the wireless router out of the box, the first thing you will notice is an Internet port and most likely four other network ports that are the switch part of the home router. The four-port switch is used to connect any wired systems you have to the network.

The first thing you should do is connect your modem from the ISP to the Internet port on the router. This will allow the router to have Internet access and will share that Internet access to the rest of the network.

### *Basic wireless router settings*

You can now connect your system to one of the four switch ports. The home router will assign your system an IP address so that you can surf the Internet, or more importantly, so that you can configure the router. To configure the router, start a web browser and type in the IP address of the router (found in the Getting Started manual). The address is most likely 192.168.0.1 or 192.168.1.1, so you would type that in the address bar of the browser.

When the browser connects to the router, you will see the configuration website of the router, where you can customize all the router settings. You need to log on to the router to make the changes. Use the username of “admin” with either no password or a password of “admin.” If that does not work, you need to check the manual for the username and password.

### *Changing default SSID*

After you are logged on, the first thing to do is to change the SSID value on the router and then disable SSID broadcasting. To change the SSID on the DIR-615 router, click the Setup link at the top and then click the Wireless Settings link on the left. In this example, you want to do a manual configuration, so click the Manual Wireless Network Setup button. The basic wireless configuration display is shown in [Figure 2-5](#).

The screenshot shows the D-Link DIR-615 router configuration interface. At the top, it displays 'Product Page: DIR-615', 'Hardware Version: B2', and 'Firmware Version: 2.23'. The D-Link logo is prominently displayed. Below the logo, there are tabs for 'DIR-615', 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The 'SETUP' tab is selected, and within it, the 'WIRELESS' section is highlighted. A sidebar on the left contains links for 'INTERNET', 'WIRELESS SETTINGS', and 'NETWORK SETTINGS'. The main content area is titled 'WIRELESS NETWORK SETTINGS' and contains the following settings:

- Enable Wireless:** ☒ Always
- Wireless Network Name:** APlus (Also called the SSID)
- 802.11 Mode:** Mixed 802.11n, 802.11g and 802.11b
- Enable Auto Channel Scan:** ☐
- Wireless Channel:** 2.422 GHz - CH 3
- Transmission Rate:** Best (automatic) (Mbit/s)
- Channel Width:** 20 MHz
- Visibility Status:** ☐ Visible ☒ Invisible

On the right side of the 'WIRELESS' section, there are 'Helpful Hints...':

- Changing your Wireless Network Name is the first step in securing your wireless network. Change it to a familiar name that does not contain any personal information.
- Enable Auto Channel Scan so that the router can select the best possible channel for your wireless network to operate on.
- Enabling Hidden Mode is another way to secure your network. With this option enabled, no wireless clients will be able to see your wireless network when they scan to see what's available. For your wireless devices to connect to your router, you will need to manually enter the Wireless Network Name on

**FIGURE 2-5:** Changing the SSID and disabling SSID broadcasting.

To change the SSID, change the Wireless Network Name setting to your desired SSID. I am using APlus. Also notice the Visibility Status setting, which you can set to Invisible to disable SSID broadcasting.

The final setting I want you to notice is an option to enable wireless, which you could deselect to disable the wireless networking aspect of the

home router. You could do this if you had no wireless systems and wanted to be sure that no one connected to your wireless network.

Don't forget to click the Save Settings button after you make changes if you want to have them saved!

### ***DHCP settings***

The next item I want to show you is how to configure the DHCP server settings of the home router. On the DIR-615, you can click the Setup link at the top and then the Network Settings link on the left. You will notice you can change the IP address of the router if you like, along with ensuring that the DHCP server is enabled (see [Figure 2-6](#)). After ensuring that the DHCP server is enabled, you can configure the range of addresses that you want the DHCP server to give out. Notice that my router is giving out 192.168.1.150 up to 192.168.1.200.

The image shows a screenshot of a router's web-based management interface. It is divided into two main sections: 'ROUTER SETTINGS' and 'DHCP SERVER SETTINGS'. The 'ROUTER SETTINGS' section includes fields for 'Router IP Address' (192.168.1.1), 'Subnet Mask' (255.255.255.0), 'Local Domain Name' (darkeworld.loc), and a checked 'Enable DNS Relay' box. The 'DHCP SERVER SETTINGS' section includes a checked 'Enable DHCP Server' box, a 'DHCP IP Address Range' from 192.168.1.150 to 192.168.1.200, a 'DHCP Lease Time' of 1440 minutes, and a checked 'Always broadcast' box.

ROUTER SETTINGS	
Use this section to configure the internal network settings of your router. The IP Address that is configured here is the IP Address that you use to access the Web-based management interface. If you change the IP Address here, you may need to adjust your PC's network settings to access the network again.	
Router IP Address:	<input type="text" value="192.168.1.1"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>
Local Domain Name:	<input type="text" value="darkeworld.loc"/> (optional)
Enable DNS Relay:	<input checked="" type="checkbox"/>

DHCP SERVER SETTINGS	
Use this section to configure the built-in DHCP Server to assign IP addresses to the computers on your network.	
Enable DHCP Server:	<input checked="" type="checkbox"/>
DHCP IP Address Range:	<input type="text" value="192.168.1.150"/> to <input type="text" value="192.168.1.200"/>
DHCP Lease Time:	<input type="text" value="1440"/> (minutes)
Always broadcast:	<input checked="" type="checkbox"/> (compatibility for some DHCP Clients)

**FIGURE 2-6:** Configuring DHCP.

### ***Setting the channel and power level***

Two additional settings you should consider changing on your device are the channel setting and the power level. Changing the channel on which your wireless network runs can help prevent interference from household devices. For example, if you find you lose your network connection when the microwave is being used, try changing the channel on the wireless router, as it may be using the same frequency range (or channel) as the microwave.

You should also consider changing the power level on the wireless access point or router so that you weaken the signal. The benefit of weakening the signal is that you can prevent someone outside the home from connecting to the wireless network.

## *Securing the wireless router*

Now I look at how to set some of the security settings I discussed, such as setting an admin password, encryption, and MAC filtering. Finally, I show you how you can lower the power level on the wireless network.

### *Admin password*

It is important to set your admin password on the router right away so that others do not log on to the router and change the settings. To change the admin password, click the Tools link at the top of the page and then type in the desired admin password (see [Figure 2-7](#)). Notice that you can configure a user password as well, which would allow someone to connect to the router and view the settings but not change anything.

**ADMIN PASSWORD**

Please enter the same password into both boxes, for confirmation.

Password :

Verify Password :

**USER PASSWORD**

Please enter the same password into both boxes, for confirmation.

Password :

Verify Password :

**SYSTEM NAME**

Gateway Name :

**ADMINISTRATION**

Enable Remote Management : ☐

Remote Admin Port :

Remote Admin [Inbound Filter](#) :

Details :

**FIGURE 2-7:** Changing the admin password.

On this page, you also have the option to allow remote administration if you want to be on the Internet and connect to your router to make changes. This is not recommended because it is more secure to ensure that someone who changes your router configuration is on the local network.

### ***Encryption***

After you change the admin password, you can then set up the encryption. Remember that you should use the more secure WPA2 if possible. To configure wireless encryption on the DIR-615, you would click the Setup link at the top of the page and then the Wireless Settings link on the left. Choose WPA-Personal as the security mode and then choose WPA2 Only in the WPA Mode drop-down list (see [Figure 2-8](#)).



**WIRELESS SECURITY MODE**

To protect your privacy you can configure wireless security features. This device supports three wireless security modes, including WEP, WPA-Personal, and WPA-Enterprise. WEP is the original wireless encryption standard. WPA provides a higher level of security. WPA-Personal does not require an authentication server. The WPA-Enterprise option requires an external RADIUS server.

**Security Mode :**

**WPA**

Use **WPA or WPA2** mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use **WPA2 Only** mode. This mode uses AES(CCMP) cipher and legacy stations are not allowed access with WPA security. For maximum compatibility, use **WPA Only**. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.

To achieve better wireless performance use **WPA2 Only** security mode (or in other words AES cipher).

**WPA Mode :**

**Cipher Type :**

**Group Key Update Interval :**  (seconds)

**PRE-SHARED KEY**

Enter an 8- to 63-character alphanumeric pass-phrase. For good security it should be of ample length and should not be a commonly known phrase.

**Pre-Shared Key :**

**FIGURE 2-8:** Configuring wireless encryption.

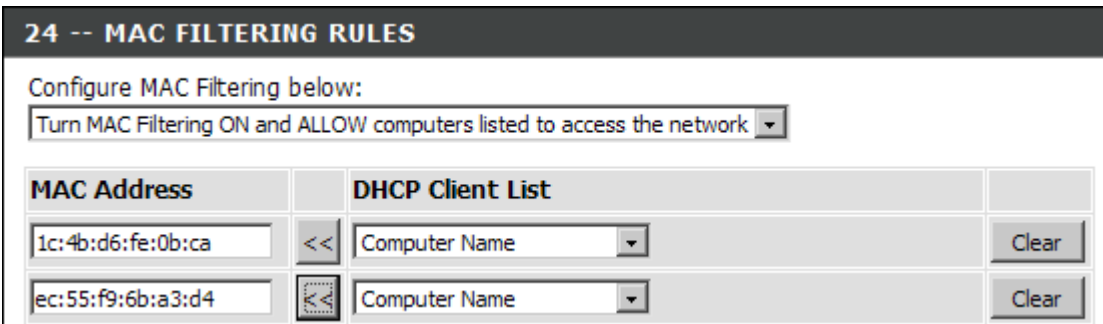
After you set the WPA mode to WPA2 Only, you then must set the password by typing the password (known as the encryption key) in the Pre-Shared Key box below. Finish things off by clicking the Save Settings button at the top of the page.

### *MAC filtering*

Another step toward securing your wireless network is to enable MAC filtering, which limits what systems can connect to the network by their MAC address. To enable MAC filtering on the DIR-615 router, you

would click the Advanced link at the top of the page and the Network Filter link on the left.

Choose the Turn MAC Filtering ON option, and then list the MAC addresses of the systems you want to allow to connect to the wireless network (see [Figure 2-9](#)).



MAC Address	DHCP Client List
1c:4b:d6:fe:0b:ca	Computer Name
ec:55:f9:6b:a3:d4	Computer Name

**FIGURE 2-9:** Configuring MAC filtering.

### *Other security settings*

You can implement a number of other settings that can aid in the security of the SOHO network. You can place the wireless access point (antenna) in the center of the building and then lower the power level of the wireless access point so that the wireless signal cannot travel as far. The goal here is to prevent someone from outside the office building from connecting to the wireless network.

You could also disable DHCP on the wireless router so that if someone does connect to the router, he does not get an IP address automatically and is then unable to network with your systems on the network. This means that you will need to assign static IP addresses to all your systems.



**FOR THE  
EXAM**

You should know these security best practices for both wired and wireless SOHO networks for the A+ exams:

- » **Change default usernames and passwords:** Ensure that you connect to the wireless router and change any default usernames (if possible) and ensure that you set passwords for the default accounts.

- » **Changing default SSID:** Change the SSID to something that has no relevance to your physical location or company name.
- » **Setting encryption:** Ensure that you enable wireless encryption to the highest level possible. For example, use WPA2, but if that is not available, use WPA.
- » **Disable SSID broadcast:** After setting the SSID value, ensure that you disable SSID broadcasting. This is known as the *visibility* setting on some routers.
- » **Antenna and access point placement:** Place your wireless access point in the middle of the building so that you can try to get equal coverage throughout the office. You may also want to ensure the antennas are located in a high place if the access point is in the basement, like on the top of a shelf.
- » **Radio power levels:** After placing the access point in the middle of the building, reduce the power level on the router so that the signal weakens after a short distance. This way, someone sitting out on the street cannot connect to your wireless network.
- » **Enable MAC filtering:** Make sure that you enable MAC filtering to limit which devices can connect to your wireless network by MAC address.
- » **Assign static IP addresses:** Although this is an administrative nightmare, in high-secure environments, you may want to disable DHCP on the router and require static addresses to be configured on any system connecting to the network.
- » **Disable ports:** The SOHO network will have wired ports on the switch. Disable any ports on the switch that are not being used to prevent unauthorized systems from connecting to the port.
- » **Provide physical security:** Ensure that the routers and switches are in a central room that is locked down to prevent unauthorized personnel from gaining physical access to the router and switches.

## *Other router settings*

You may want to check out a number of other settings on the wireless router. The following are some settings worth knowing for the A+ exams:

- » **Update firmware:** It is important to ensure you update the firmware on the wireless access point or router to ensure that you have the most up-to-date features and bug fixes for the device.
- » **Channels:** If you find that you keep losing your wireless connection, it could be because other household devices like a cordless phone are interfering with your wireless. You can change the channel of the wireless network, which places it on a different frequency.
- » **Firewall settings:** The home router typically has a firewall feature that is enabled by default. This firewall prevents traffic from the Internet from entering your network.
- » **Port forwarding/mapping/triggering:** If you are hosting a web server or gaming server, you may need to open ports on your firewall with the port forwarding/triggering feature. When setting up port forwarding, you specify what port to open on the firewall and then the IP address to send that traffic to. You can also create port mappings where a specific port outside the firewall is forwarding to a specific system and port number on the inside of the network.
- » **DMZ:** Most home routers give you an option to configure a DMZ (demilitarized zone), which is a system that can receive limited traffic from the Internet.
- » **Content filtering/parent controls:** Most wireless access points and routers provide a number of features to limit the types of sites users can visit by creating content filters. Content filters may involve denying access to certain URLs or denying access to certain keywords. Most wireless routers today also have parent controls with which you can control the times of day different users or devices are allowed Internet access.
- » **UPnP:** *Universal Plug and Play* (UPnP) is a networking feature on many types of devices such as computers, printers, mobile devices, and wireless access points that allow the device to locate one another on the network and share services such as files.

- » **NAT/DNAT:** *Network Address Translation* (NAT) is a feature that allows an Internet connection to be shared among multiple computers or devices. NAT is the feature of a wireless router that allows you to have one public IP address assigned to one network card on the router so that all systems gain access to the Internet through the one IP address.
- » **WPS:** WiFi Protected Setup (WPS) is a feature that allows you to easily configure wireless security settings such as SSID and encryption, while only requiring users to connect using a PIN.
- » **Basic QoS:** Quality of service allows you to control bandwidth utilization on the network. This allows you to ensure that a certain application is not using all your network bandwidth.

## *Other Wireless Connections*

Two more products fall into the wireless networking category: Bluetooth and cellular. Bluetooth is used as a communication link between different devices, and cellular is used for remote dial-up networking or Internet access. In both cases, using these wireless devices is very different than the 802.11 wireless networking protocols, which are designed to be a short-range extension of a LAN (local area network).

### *Bluetooth*

Bluetooth follows the standards set out in the IEEE 802.15 specification. As a personal area network (PAN), Bluetooth is designed primarily for use in very small areas or short ranges, such as on a person's body. You have probably seen cordless cellular phone headsets, which operate over the space between the headset in the ear and a phone carried on the hip or in a purse. Most wireless links for today's cellphones and PDAs use Bluetooth. You might not immediately think of these links as being on a network — after all, you are not surfing the Internet or transferring files — but you are transferring data, in some form, between the devices. There are three classes of devices on Bluetooth networks:

- » **Class 1** devices operate at 100 milliwatt (mW) and have a range of 100 meters.
- » **Class 2** devices operate at 2.5 mW and have a range of 10 meters.
- » **Class 3** devices operate at 1 mW and have a range of about 1 meter.



**REMEMBER** Most devices are Class 3. Class 3 Bluetooth devices include telephone and computer headsets, PDA-to-PC synchronization, printers, digital cameras, cellphones for synchronizing with PCs, game controllers, remote controls, and instrument collection devices.

Bluetooth has replaced serial or infrared connections that would have been used for many of these functions in the past. Bluetooth is used mainly in low-bandwidth, short-haul situations.

Bluetooth operates in the 2.4 GHz spectrum, specifically around the 2.45 GHz mark. This means that it is open to interference from other devices running in the same spectrum. However, because of its limited range, it tends to cause fewer problems with devices that are outside of its range.

Some Bluetooth devices have a security feature — pairing — that can and should be used when available. There have already been viruses affecting Bluetooth cellphones that were originally set to freely associate with any other Bluetooth device in the area. Most phones now require pairing with devices to communicate.

*Pairing* registers a pair of devices with each other by using a shared secret key so that they can talk only with other devices that are known. Pairing is used as a means of authentication between devices and can also be used to encrypt data communication between them. Some devices, such as printers, might end up being left open and unsecured to keep a high level of functionality, but this would be a conscious decision to leave pairing turned off, and to leave the device unsecured.

## ***RFID, IR, NFC, ZigBee, and Z-Wave***

Radio frequency (RF), infrared (IR), and *near field communication* (NFC) are common wireless technologies that allow you to have devices communicate with one another without the use of a physical cable. RF is the wireless communication method used by wireless networks such as 802.11g/n/ac. RF uses electromagnetic frequency waves for communication.

IR is a wireless technology that communicates data through infrared radiation, which is information at a wavelength longer than that of a red light. IR is commonly used with home entertainment remote controls and is a line-of-sight technology, meaning that there cannot be any obstruction between the two devices communicating.

NFC is a newer form of wireless communication that allows two devices to exchange information when the devices are placed closely together (within 4 inches). This is common today with bank cards being able to make payments or a smartphone being able to exchange data with another device.

NFC devices, such as smartphones, can operate in three different modes. NFC card emulation mode allows the NFC device to act like a smartcard that can be used to make payments for a purchase. NFC reader/writer mode is used to read information from an NFC tag that is on a label or smart poster. And finally, NFC peer-to-peer mode allows any two NFC devices to communicate with one another and exchange information.

Zigbee is a wireless communication protocol that is designed to replace Bluetooth as it is less expensive to implement. Zigbee has the same characteristics as Bluetooth in the sense that it is used in scenarios where devices are in close proximity and require little power and bandwidth to communicate data with one another. Zigbee is the perfect communication protocol for home automation devices. It is a line-of-sight technology that has a maximum distance of 100 meters at a data transfer rate of 250 Kbps.

Another common wireless communication protocol using radiowaves (not line-of-sight) used by home automation devices is Z-wave. Z-wave uses wireless communication in a mesh topology and is perfect for low-bandwidth scenarios. Z-wave allows you to control home automation

devices such as lighting, security systems, and appliances. Z-wave also allows for transfer rates of up to 100 Kbps with a distance of 100 meters.

### ***WAN cellular and cellular networks***

A wide area network (WAN) — unlike a LAN, which is contained within one or two adjacent buildings — spans a large geographical area and usually involves communication links operated by a Telco. Considering the number of communities and cities planning to set up wide-scale public access wireless networks and the cost of cellular data transfer rates, WAN cellular technology might not become extremely widespread.

### ***WAN cellular***

In conjunction with your data network provider, you can sometimes get cellular WAN access to your network: wireless wide area network (WWAN). You need a special cellular gateway or a data-enabled phone, which some people might refer to as a modem. Unlike a normal cellular modem that needs to dial another modem to establish a connection, the gateway makes a connection directly to the cellular provider's network. The gateway may be connected to your computer by USB, Bluetooth, or PCMCIA. This gateway connects to your data network provider and sets up a secure tunnel for access to your corporate network's resources. The data rates on these connections are usually faster than traditional dial-up connections, and they do provide secure access to your LAN data services, but most service providers charge a substantial fee for the service.

### ***Cellular networks***

Another form of wireless communication that cannot be ignored is the wireless network being used by mobile devices such as phones and tablets that you subscribe to. These technologies are used by the service providers to give your phone or tablet Internet access. The following are cellular network technology used by service providers:

- » **3G:** An older standard for mobile device communication that had a transfer rate anywhere from 400 Kbps to 2 Mbps, depending on the version of 3G technology used.



- » **4G:** The next generation of mobile communication provides Internet access with transfer rates typically between 20 Mbps and 50 Mbps, but a potential of up to 100 Mbps.
- » **LTE:** Long Term Evolution (LTE) is marketed as a newer version of a 4G technology that provides a transfer rate of up to 300 Mbps.
- » **5G:** The fifth generation of the mobile network provides Internet access with a huge boost in bandwidth with a potential transfer rate of up to 10 Gbps!

## *Increasing Wireless Network Performance*

Some basic steps that you can take to improve wireless performance include the following:

- » **Reduce interference from other sources.** This might include changing channels that you are using or changing the spectrum that you are using, such as switching from 2.4 GHz to 5 GHz technologies.
- » **Reduce the number of clients per access point.** Because wireless is a shared medium, the fewer clients the access point has to share bandwidth between, the faster each client will be.
- » **Reduce the range between the clients and the access points.** As the range between the client and access point increases, the signal quality decreases — and, therefore, the data throughput rate decreases.
- » **Use faster technology.** For example, upgrade from older wireless technologies such as 802.11g to either 802.11n or 802.11ac.
- » **Reduce the material that the signal must travel through.** The distance ratings are usually open-air ratings, and construction materials and other objects in the path of the signal will reduce the signal strength.



**REMEMBER** Outdoor wireless networks set up during the winter can experience problems in the spring when trees in the path of the signal leaf out. Try to anticipate how annual weather and seasonal changes in your area will affect both your wireless equipment and wireless signal.

- » **Use proprietary or nonstandard technology to improve data transfer speeds.** This might work only when teamed with specific network cards from the wireless vendor.

## *Troubleshooting Issues*

Any issues that affect wired networks can affect wireless networks as well. Very often, symptoms show up first on the wireless network. The bandwidth on the wireless network is substantially lower, so when a problem on your network consumes bandwidth — like a worm — it will cause connectivity and performance issues on your wireless network before users of your wired network notice the problem.

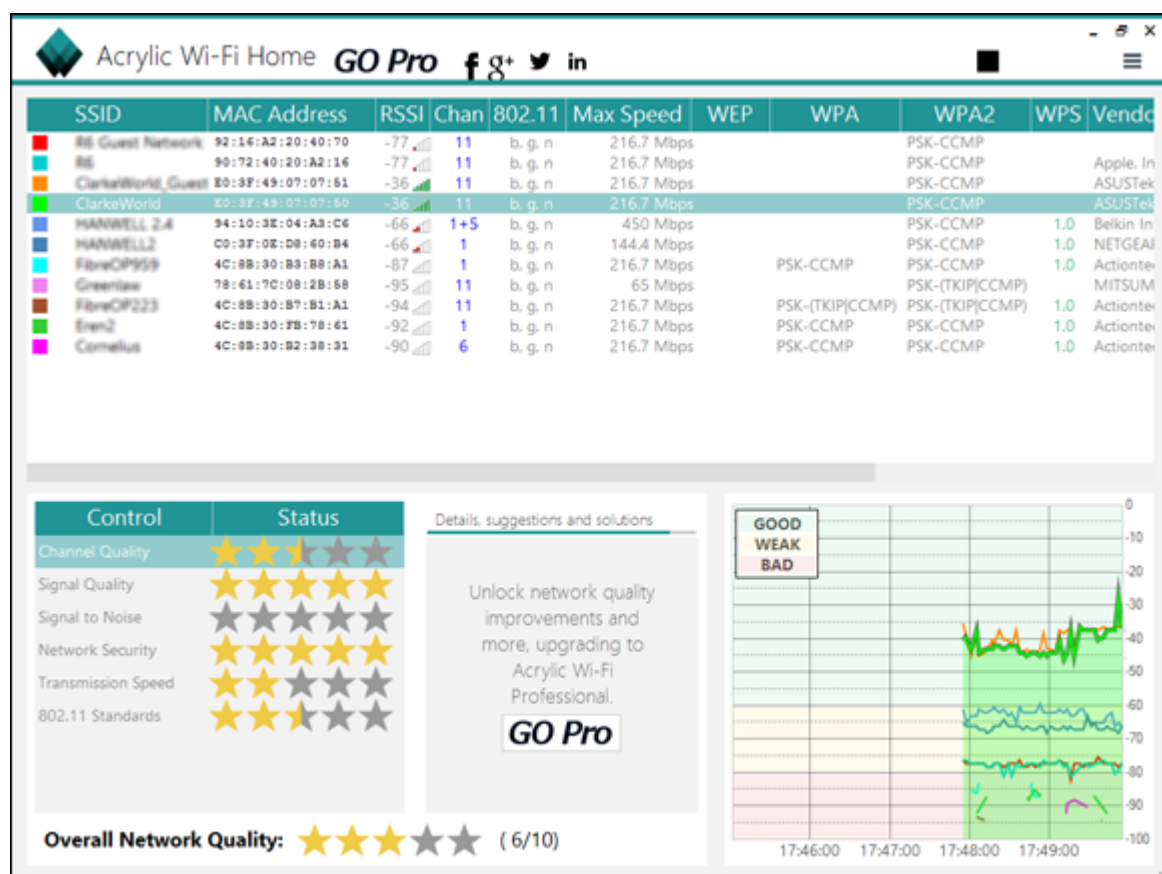
### *Low RF signal*

A number of outside factors, such as microwaves and cordless phones, can affect wireless networks and give you a low RF signal. Remember when troubleshooting signal issues, you can change the channel on your wireless access point, which places your wireless network on a different frequency in hopes to reduce the interference and gain a stronger signal.

When assessing wireless networks, you can use a wireless scanner to view all the wireless networks and channels being used. Because microwaves and cordless phones operate throughout and beyond the 2.4 GHz spectrum, and because they do not advertise themselves as wireless networks, they won't show up in the results of your wireless scanner software when you are viewing the strength of wireless networks in the area. To locate these rogue signals, you need to perform a physical inspection — or, better yet, run a spectrum analysis tool. These tools used

to cost thousands of dollars, but the price of quality tools has dropped to hundreds of dollars, and some tools cost even less. Managing your wireless frequencies is becoming just as important as managing your wired data networks.

To survey wireless networks in your area so that you can choose a clear channel, use a wireless scanner such as WiFiInfoView or Acrylic WiFi scanner. You can use these tools to view detailed information about the wireless networks and signal information within your area. Looking at [Figure 2-10](#) you can see the different SSIDs of wireless network, the MAC address of the access point, the strength of the signal, the channel being used, maximum speed, and whether WPA or WPA2 is being used. When you select an SSID, it gives you a rating that represents your channel quality, signal quality, and network security. Many other applications do the same type of thing, and this feature is even incorporated into the management software that ships with some network card drivers.



**FIGURE 2-10:** Use Acrylic WiFi scanner and similar tools to see wireless networks in your area.

## *SSID Not Found*

If you are having trouble connecting to a wireless network because you cannot see the name of the wireless network in the list of networks to connect to, it could be because the SSID is not being broadcasted by the wireless access point. In this case, you should be able to type the name of the SSID (if you know it) and then connect. When typing the name of the SSID, know that it is case-sensitive.



TECHNICAL  
STUFF

If you know that an access point is not broadcasting its SSID, you can find the SSID by using wireless network auditing tools, like Kismet found in Kali Linux which you can download from

[www.kali.org](http://www.kali.org).

## *Security settings*

If you can get a good signal but you don't seem to be able to establish a connection or transfer data with the network, look at the security settings on both the access point and the client computer. If the WEP settings are incorrect or if the network authentication is not set correctly, you might experience either of these problems.

Much the same as WEP keys and settings, if you are using WPA, your problems could be with the shared secret that is configured or the settings for the authentication server, which verify user or access point credentials.

## *Getting an A+*

This chapter goes over some common wireless communications. The following points are covered:

- » Infrared technology depends on line-of-sight and tends to be used for low-bandwidth solutions.
- » A number of factors affect wireless signal quality and strength, such as interference, range, and the number of connected clients.
- » 802.11a/b/g networks all have a range of 100 feet (30 meters), and 802.11n has a range of 165 feet (50 meters). 802.11a networks operate in the 5 GHz spectrum, and 802.11b and 802.11g networks operate in the 2.4 GHz spectrum; 802.11n networks can operate in both spectrums.
- » WEP and WPA are the most common methods to secure wireless networks, but other options include disabling SSID broadcasting, MAC filtering, placing wireless APs in a DMZ, and changing default passwords.
- » Bluetooth is used only for short-range communication.

## *Prep Test*

**1. Which of the following is not a technology that can be used to connect to a printer?**

- (A) Bluetooth
- (B) WWAN
- (C) 802.11b
- (D) Infrared

**2. Typical client Bluetooth implementations have what ranges? (Select all that apply.)**

- (A) 1 meter
- (B) 5 meters
- (C) 10 meters
- (D) 25 meters

**3. What is the standard range of 802.11a/b/g wireless networks?**

- (A) 10 meters
- (B) 30 meters
- (C) 50 meters
- (D) 100 meters

**4. Which of the following does *not* impact the quality of wireless signals?**

- (A) Microwave ovens
- (B) Air temperature
- (C) Cordless phones
- (D) Distance between access point and clients

**5. 802.11g networks are backward compatible with which other 802.11 technology?**

- (A) 802.11a
- (B) 802.11b
- (C) 802.11i
- (D) 802.11n

**6. Which of the following would be used to provide wireless connectivity across a metropolitan area?**

- (A) Bluetooth
- (B) Infrared
- (C) Cellular
- (D) MIMO

**7. What frequency ranges are used by 802.11 wireless networks? (Select all that apply.)**

- (A) 900 MHz
- (B) 1.5 GHz
- (C) 2.4 GHz

- (D) 5.0 GHz
- 8. You are a network technician for your company and are working on securing your wireless network environment. Which of the following is considered the weakest security method?**
- (A) WPA2
  - (B) WEP
  - (C) WPA
  - (D) 802.11i
- 9. As the network technician you are looking to control which client systems are able to connect to the wireless network. What wireless security feature will you use?**
- (A) MAC filtering
  - (B) Port forwarding
  - (C) Content filtering
  - (D) WPA2
- 10. One of your users has called you asking for advice. He is setting up a small office/home office (SOHO) network and would like to configure the network so that his neighbors cannot see the network. Which of the following should be done?**
- (A) Enable SSID broadcasting
  - (B) Enable firewall filtering
  - (C) Disable SSID broadcasting
  - (D) Enable WPA2s

## *Answers*

1. **B.** Printers from different manufacturers support some of or all the listed wireless technologies, and WWAN is a technology used to connect to your network while out of the office. See “[\*Understanding\*](#)

[Infrared Devices](#), ” [Bluetooth](#), ” and [Working with Wireless Networks](#). ”

2. **A, C.** Bluetooth technology has ranges of 1, 10, and 100 meters depending on the class of devices that are being used. Review [Bluetooth](#). ”
3. **B.** Most 802.11 wireless networks have a range of 30 meters in open air. Check out [Wireless standards and protocol](#). ”
4. **B.** Air temperature has not been documented to have an impact on wireless networks. Peruse [Troubleshooting Issues](#). ”
5. **B.** 802.11g uses the same 2.4 GHz spectrum and was designed to be backward compatible with 802.11b. 802.11n is backward compatible with both 802.11g and 802.11b. Take a look at [802.11g](#). ”
6. **C.** The only technology that will work across a metropolitan area is cellular, which is used for WAN cellular or WWAN connectivity. Peek at [WAN cellular](#). ”
7. **C, D.** 802.11 networks run at either 2.4 GHz for 802.11b/g/n or 5.0 GHz for 802.11a. Look over [Wireless standards and protocol](#). ”
8. **B.** WEP is considered the least secure security protocol when it comes to wireless networks. Study [Securing wireless networks](#). ”
9. **A.** MAC filtering is a feature of wireless access points that allows you to control which clients can connect to the wireless network by their MAC address. Study [Securing wireless networks](#). ”
10. **C.** To configure the wireless network so that it is not easily found, you would disable SSID broadcasting. Study [Securing wireless networks](#). ”



# Chapter 3

## Networking the Operating System

---

### IN THIS CHAPTER

- » Identifying network protocols
  - » Configuring the TCP/IP protocol
  - » Troubleshooting with TCP/IP utilities
  - » Understanding name resolution
  - » Sharing network resources
  - » Understanding Windows Services
- 

One of the most important skills IT professionals need to master is troubleshooting networking connectivity: that is, computers establishing a connection with one another. A number of components facilitate this communication, and many times, IT professionals end up troubleshooting issues with these components.

This chapter discusses the software components that allow a computer to network with other computers as well as the troubleshooting issues that could arise while configuring a network. In this chapter, you find out how to connect to networking resources and how to troubleshoot when you cannot make the connection.

## *Understanding Networking Components*

When setting up a network, you must have the appropriate hardware and software in place to allow systems to communicate with one another.

Because this chapter focuses on the software components needed to allow Windows to network, you can assume that you have all the necessary hardware in place. You have a hub or switch, at least two computers and network cards to go in the computers, and the appropriate cabling to connect the network cards to the hub/switch is already connected. After all the hardware is in place, consider what you have to do at the operating system level to get these computers talking. Not only do you need the physical hardware in place but you also need to load software components, such as a network card driver, protocol, service, and client software. These are the four major software components required to network.



**REMEMBER** When building your network, it is important to identify the four major software components that allow a Windows OS to function in a networking environment:

- » Network adapter driver
- » Network client
- » Protocol
- » Services



**FOR THE EXAM** I discuss each component in detail in the sections that follow. Be sure you are comfortable with them for the A+ exams!

## ***Network adapter driver***

The *network adapter driver* is the physical network card inserted into one of the computer's expansion bus slots, connected as a USB device, or integrated into the system board. The network card is responsible for sending information onto the network and receiving information from the network.

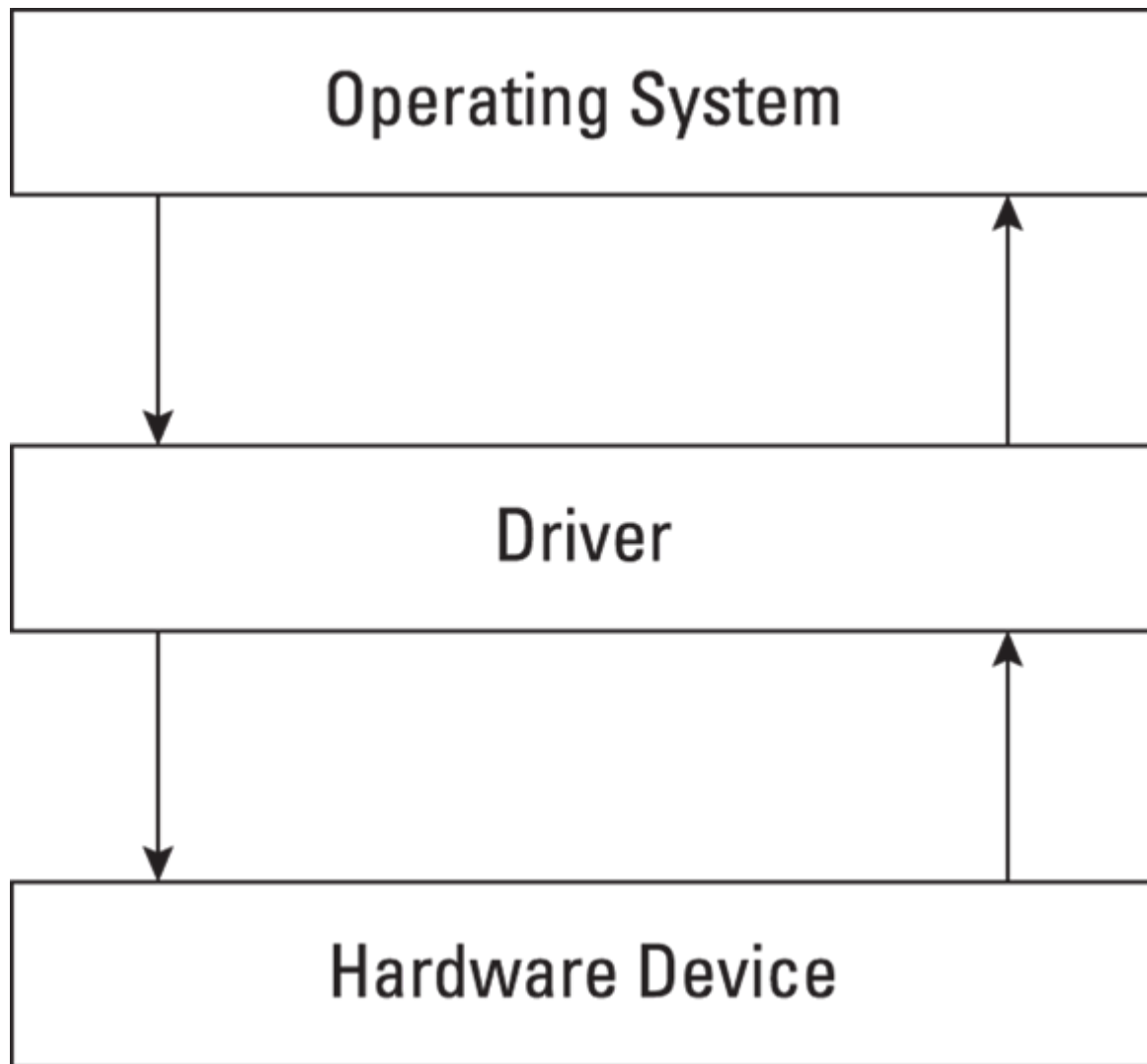
Before purchasing a network card, you have to figure out what type of card you need. To do this, open the computer (for more information on safety procedures, refer to Book 1, [Chapter 3](#)), look at the expansion buses supported in your system, and then identify which has an empty slot. For example, if you have a PCI slot and a PCIe, you can choose between a PCI or a PCIe network adapter. Typically, you would opt for the PCIe network adapter because of the performance benefits of PCIe devices over PCI devices.



**TIP**

A USB network adapter is a popular choice today. If you go with a USB network adapter, you won't need to open the computer — simply plug the USB adapter into an available USB port.

After you install the network card into the empty expansion slot or USB port, you install the driver for that card within the OS. Installing the network card driver is the first major step to networking a system because the driver software allows the OS to communicate with the physical device — in this case, the network card. [Figure 3-1](#) shows how the driver sits between the OS and the physical hardware, controlling communication between the two.



**FIGURE 3-1:** The relationship between the OS and a hardware device is controlled by the device driver.

### *Installing a network adapter in Windows*

After you insert the network card into the computer, Plug and Play will kick in when the computer is powered on. If the OS has the device driver for the card, it will load the driver automatically, and you will see the device listed in Device Manager.

If the OS doesn't have the driver, it will either prompt you for the driver (and then you need to supply the manufacturer's CD for the network card), or the device will be listed in Device Manager as an unknown device. To update the driver for the device in Windows, go to Device Manager to

update the driver. The following steps demonstrate how to update a driver in Windows:

- 1. Click Start, right-click Computer, and choose Properties in Windows 7, or right-click the Start icon and choose System in Windows 8.1/Windows 10.**
- 2. In the System Properties dialog box, click the Device Manager link on the left.**

The Device Manager appears.
- 3. Within Device Manager, expand Network adapters and right-click your network card.**
- 4. To update the driver, choose Update Driver, as shown in [Figure 3-2](#).**

If your network card isn't listed in the Network Adapters section of Device Manager, look under the Unknown Devices category. If the device is in the Unknown Devices category, right-click it there and choose Update Driver.

The Update Driver Wizard starts.
- 5. Select Install from a List and then click Next.**
- 6. Select Don't Search, I Will Choose the Driver to Install; then click Next.**
- 7. Select the manufacturer of your network card (on the left) and then choose the model of your network card (on the right). Click Next.**

If your network card model isn't in the list, click the Have Disk button so that you can supply the location of the driver.
- 8. After the driver is copied, click Finish.**



**FIGURE 3-2:** Updating a network card driver in Windows.

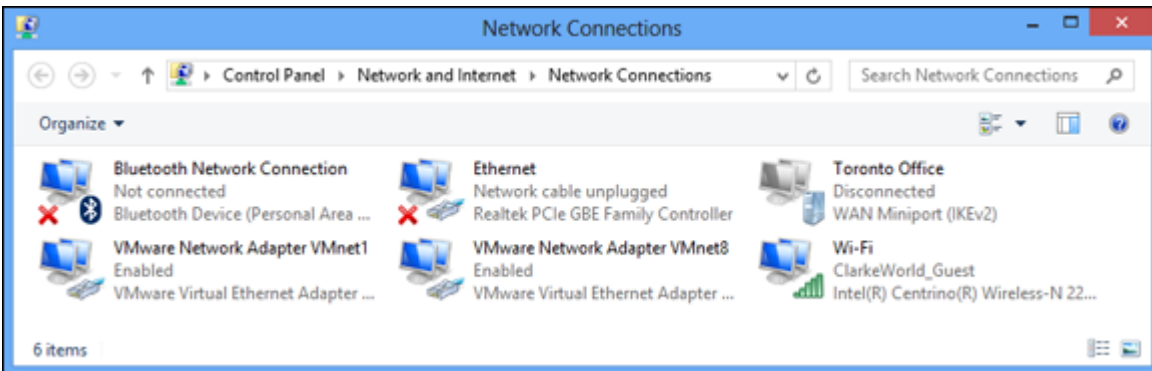
### *Understanding network connections*

After you load the network card driver, Windows creates an icon that represents the network card; this icon is called a *network connection*. If you have multiple network cards installed, you have multiple network connections — one representing each network card.

The purpose of the network connection icon is to give you a place to configure any network settings responsible for communication between the network card and the local area network (LAN). For example, if you want to ensure that TCP/IP is used by your network card, right-click the local area connection and choose Properties. In the Properties of the network connection, you can add or configure networking components, such as TCP/IP.

To view your network connections in Windows, choose Start ⇒ Control Panel (in Windows 7) or right-click the Start icon and choose Control Panel if using Windows 8.1. Once in the Control Panel, choose Network and Internet ⇒ Network and Sharing Center.

The Network and Sharing center is the main screen for viewing or changing your network settings. To see the different network connections, choose the Change Adapter Settings link on the left side of the screen. You'll see a window that displays your network connection icons, as shown in [Figure 3-3](#). Each of these network connections is there because of a network card driver being installed for your network interfaces.



**FIGURE 3-3:** Viewing local area connection in Windows.

When you right-click the local area connection icon, its contextual menu gives you a number of tasks. Here are tasks that you might use when you troubleshoot networking issues:

- » **Disable:** Temporarily cut off communication to and from the network. This is a quicker solution than physically removing the network card from the computer.
- » **Enable:** This choice is a toggle of Disable when you disable a card. After you troubleshoot your network (hopefully, you fix the problem) and you need to re-enable the network connection, choose Enable.
- » **Status:** Display a dialog box showing how long the connection has been up and running and also the speed of the connection. On the Support Page tab, you can view your IP (Internet protocol) address information and MAC (Media Access Control) address.
- » **Diagnose:** Have Windows perform maintenance on the connection by performing tasks such as renewing your IP address, flushing the ARP (Address Resolution Protocol) cache, and flushing the NetBIOS and domain name system (DNS) resolver cache.

- » **Rename:** Give the connection a more meaningful name. For example, I renamed the LAN for the network card connected to the Internet to *Internet Connection*.
- » **Properties:** Open the Properties dialog box for your LAN connection. In the Properties dialog box, you can modify the network setup of the network card. For example, you can add or remove network protocols or change their configuration.

After you make sure that the correct hardware settings are applied to the network adapter, your next step is to connect to a network resource. Unfortunately, you cannot connect to a network resource until you have the appropriate network client running. The following section describes the purpose of the network client.

## *Network client*

In essence, a network client is no different than a client or customer in the real world. A client in the real world visits your company because you provide some sort of service. Say you run a tailor shop. The customer is a *client* of the tailoring service.

Computer networks work the same way. On your computers, you must run a client for the type of service you are requesting on the network. For example, if a company runs the older Novell NetWare as the server OS, you must load a client that will connect your computer to the Novell server. Or, if you want to connect to a Windows server, you have to load a Microsoft client on your system.

The Windows OSes come with the Client for Microsoft Networks already installed so that you can automatically connect to a Windows network.

To return to my tailor shop example, say that your client asked your service to tailor some pants. When the client finally receives the mended pants, that client is pleased — however, the pants have to be dry-cleaned before they are used. Unfortunately, your business doesn't offer dry-cleaning services, so your client has to request that service from a third party. The point is that your client can be a client of tailoring *and* a client



of dry cleaning at the same time. There is no rule that says you can be a client of only one particular service at a time.

To install a network client for Microsoft networks in Windows, follow these steps:

**1. Locate the network connections:**

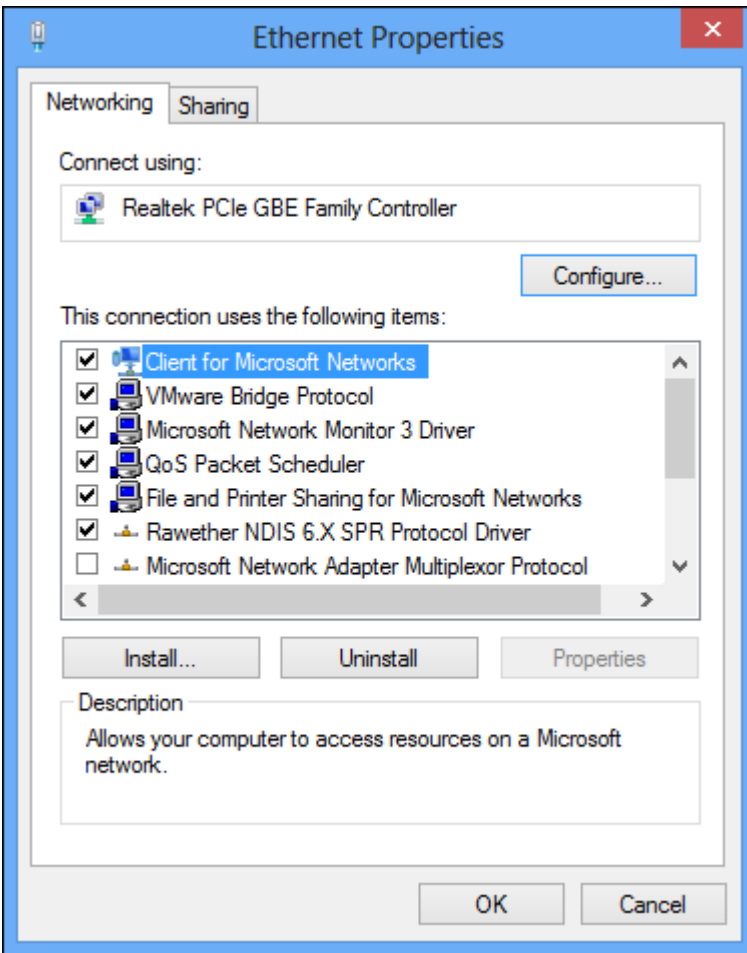
- *Windows 10:* Click the Start button, then type **control**. Choose Control Panel from under the Best Match section. Choose Network and Internet ⇒ Network and Sharing Center ⇒ Change Adapter Settings.
- *Windows 8.1:* Right-click the Start icon and then choose Control Panel ⇒ Network and Internet ⇒ Network and Sharing Center ⇒ Change Adapter Settings.
- *Windows 7/Vista:* Click Start ⇒ Control Panel ⇒ Network and Internet ⇒ Network and Sharing Center, and then click the Change Adapter Settings link on the left.

**2. Right-click the network connection, which should appear as Ethernet (Windows 8.1/Windows 10) or local area connection (Windows 7), and then choose Properties.**

**3. If it isn't already active, click the General tab.**

**4. Verify that Client for Microsoft Networks appears in the list of components and has a check mark beside it, as shown in [Figure 3-4](#).**

If the check box is not selected, select the Client for Microsoft Networks check box to enable the Microsoft networking client. If the Client for Microsoft Networks is not in the list, install it: Click the Install button and choose Client from the Network Component Type dialog box. Click Add, choose Client For Microsoft Networks, and then click OK.



**FIGURE 3-4:** Verify that Client for Microsoft Networks is installed.

At this point, you should have your network card and its driver installed, and you should also have installed the appropriate client. Unfortunately, you still cannot communicate with someone on the network because you still have to install the appropriate protocol. In the following section, I talk about the purpose of protocols and what common protocols are running on networks today.

## ***Protocols***

*Protocols* are languages used to hold a conversation on a network. Your system can have a network card installed and have the proper client running, but if it is not speaking the same language (um, protocol) as the remote system, the two systems cannot hold a conversation. Back to the tailor shop example: You are now ready to service your clients, but you have a teeny problem. The first client who walks into your store and

requests service speaks French, but you speak only English. To solve this problem, you and your client must speak a common language — and it doesn't matter what that language is, as long as you both can speak it.



FOR THE  
EXAM

There are a few things to look for when choosing which protocol to install, but the bottom line is that all computers on the network must have the same protocol installed — a common denominator to allow all individuals to participate in a conversation. In the following sections, I discuss a few different protocols that you might encounter when working with networks. Be sure you are familiar with these protocols when you take the A+ certification exams.

### ***NetBEUI***

*NetBIOS Extended User Interface* (NetBEUI) was originally developed by IBM to be used on small networks (fewer than ten computers).

Microsoft implemented NetBEUI in the different Windows OSes for the same purpose — small networks — because it is a *nonroutable* protocol, meaning that it cannot leave the network. Because many companies have large networks spanning some form of wide area network (WAN) link and containing routers to connect different networks, this protocol is impractical in those environments and for environments that want to connect to the Internet.

In the past, you would use NetBEUI if you had a small number of computers that needed to be networked in a workgroup-type environment. You wanted to get this network up and running without the hassle of having to configure all kinds of settings. This is the benefit of NetBEUI: There is no configuration — it just works! In today's networking environments, though, seeing NetBEUI on any major network is unlikely.

### ***TCP/IP***

*Transmission Control Protocol/Internet Protocol* (TCP/IP) is the hot protocol on the market these days because it is the protocol of the Internet and Internet-based technologies. TCP/IP has become the protocol of

choice for Windows, Linux, and Novell networks because of its ability to communicate in heterogeneous environments. The bottom line is this: It doesn't matter what kind of OS you are running — if you're running TCP/IP, you can communicate globally.

TCP/IP is a protocol suite. *Protocol suites* are like application suites in the sense that there is more than one protocol in the group. For example, if you purchase the Microsoft Office suite, you purchase an entire group of applications, or an entire *suite* of applications. TCP/IP is a group of protocols that make up the protocol suite, and some of these protocols are used day in and day out. For example, adding the TCP/IP protocol suite to your computer means that you have a Telnet application for running applications from another computer, and you have an FTP application for downloading files from another computer.

Because configuring TCP/IP is such a big topic, I devote an entire section of this chapter, "[The TCP/IP Protocol](#)," to it.



FOR THE  
EXAM

TCP/IP is a routable protocol, and NetBEUI is a nonroutable protocol.

## Services

One of the most forgotten networking components is the *service*, which is a piece of software running on the computer that provides certain functionality. An example of a service that runs on the computer is file and printer sharing, which is the service that provides files, folders, and printers to other systems on the network.

Going back to the tailor shop example: Before you can have clients, you must have first made the decision to offer the service. If you do not offer the service, there is no reason for customers to want to communicate with you.

So, on a network, someone has to offer the service, but not everyone needs to. For example, a small company with five Windows machines might have only the machine with the printer connected to it providing the

File and Printer Sharing service. The other four Windows computers connect to it by installing Client for Microsoft Networks and ensuring that they are using the same protocol. There is no reason for them to have the service installed because they are offering nothing to the network.

Windows servers usually run at least two services by default:

- » **File sharing services:** Allow the server to share files with other users on the network.
- » **Printer sharing services:** Allow a printer to be used by multiple users on the network. You don't need to purchase a separate printer for each user on the network, which is a real cost cutter!

File and Printer Sharing services were the original purpose in life for servers and networks, but the number of services that can be added to these systems has grown over the years to include mail services, web services, FTP services, name resolution services, and many more.

## REAL-WORLD SCENARIO: PLANNING NETWORK COMPONENTS

You are responsible for determining what networking components are required in order to build the following scenario. The answer follows the scenario.

**Scenario:** You are in charge of implementing the network infrastructure for your organization. There are two Windows Server 2012 R2 servers and three Linux servers servicing 200 Windows 8.1 clients. The word processing department will be sending print jobs to one Windows 8.1 computer in the manager's office. What networking components would you load to allow the clients to access both the Linux servers and the Windows Server 2012 R2 servers?

**Answer:** The Windows 8.1 computer in the manager's office will have File and Printer Sharing for Microsoft Networks loaded so that the Windows 8.1 clients in the word processing department may connect to it and submit print jobs.

You will have to load a Linux client so that the Windows 8.1 clients can connect to the Linux servers. You will also have to ensure that all clients are configured with TCP/IP.

To allow the Windows 8.1 clients to connect to the Windows Server 2012 R2 servers, you need to ensure that the Client for Microsoft Networks is loaded, which it is by default.

# *The TCP/IP Protocol*

Since the dramatic growth of the Internet, TCP/IP has become the preferred protocol on networks today. TCP/IP is the common protocol on all desktops — including Windows, Linux, and Mac systems — allowing all these different OSes to communicate over a common protocol. It doesn't matter what OS you run or what kind of network you have: As long as you are running a common protocol such as TCP/IP, you can access resources across any platform.

TCP/IP is installed by default with every major OS (Windows, OS X, and Linux). When configuring TCP/IP on these systems, three major settings need to be configured to allow the computer to communicate with other computers on different networks or the Internet:

- » IP address
- » Subnet mask
- » Default gateway

To troubleshoot communication across TCP/IP, you need to understand the types of settings that need configuring. In the sections that follow, you look at how to configure TCP/IP and at some utilities to help you troubleshoot the protocol.

## *IP address*

The *IP address* is a 32-bit number that is unique to your computer. No two systems can have the same IP address. An IP address is similar to the address of your home, which is the method by which other people send mail to you. An IP address works the same way on a TCP/IP network: You assign the number to your computer, and it is the method other computers use to send information to your computer.

An IP address is made up of four sets of numbers separated by periods: dotted decimal notation format. Here's an example:

```
131.107.2.200
```

Each of the four sets of numbers represents an *octet* (because each octet represents 8 bits of data).

The IP address comprises a network ID and a host ID:

» **Network ID:** This unique number is used only by your network and is also the same for all computers on the same network.

For example, in the IP address 131.107.2.200, the first two octets (131.107) make up the network ID. So if computer A with an IP address of 131.107.2.200 talks to computer B with an IP address of 131.107.3.5, you can assume that the two computers are on the same network because 131.107.x.y is the network ID for both computers.

» **Host ID:** This portion uniquely identifies a computer on the network.

For example, in the IP address 131.107.2.200, the last two octets (2.200) make up the host ID. Only one computer on the 131.107.x.y network can have the host ID of 2.200.



**WARNING** The network ID is not always the first two octets of the IP address. So how do you know which octets make up the network ID and which octets make up the host ID portion of the IP address? The *class* of IP address you have dictates which numbers correspond to which IDs. The three major classes of IP addresses are Class A, Class B, and Class C. The different IP address classes support a different total number of workstations on the network. For example, a Class A network (a network using Class A addresses) supports as many as to 16,777,214 network devices, a Class B network supports 65,534 network devices, and a Class C network supports only 254 network devices.

Class A networks use the first octet as their network ID and the remaining three octets as the host ID. A Class B network uses the first two octets for the network ID and the last two octets as the host ID. A Class C network uses the first three octets as the network ID and the last octet for the host ID.



FOR THE  
EXAM

How do you know what class IP address you have? Look at the first octet. If it has a value between 1 and 127, it's a Class A IP address; if it has a value between 128 and 191, it's a Class B IP address; and if it has a value between 192 and 223, it's a Class C IP address. [Table 3-1](#) summarizes IP address classes.

**TABLE 3-1 IP Address Classes**

<i>Network Class</i>	<i>Number of Hosts</i>	<i>Octet Summary</i>	<i>First Octet Value</i>
Class A	16,777,214	n.h.h.h*	1–127
Class B	65,534	n.n.h.h	128–191
Class C	254	n.n.n.h	192–223

\* *n* = network, *h* = host



TECHNICAL  
STUFF

In the Number of Hosts column, two numbers are missing. For example, a Class C address *could* have 256 possible addresses, numbered 0 through 255. However, you are not allowed to use 0 because it is reserved for the network ID. Also, you are not allowed to use the 255 because it is the broadcast address, which is how systems send data to every computer on the network. To summarize, with each address class, you lose two addresses because of the network ID and the broadcast address.

It is important to note that no system or device can start with an IP address of 127 in the first octet. This is because it is illegal for a system on the network to have an IP address that starts with 127 as it is a reserved address. Any address starting with 127 is illegal because this address is reserved for the *loopback address*, which is an address that always refers to the TCP/IP software stack that initialized on *your* system. Typically, the loopback address is referred to as 127.0.0.1, but you could use any



address that starts with 127. For example, you could issue the following command in a command prompt to test that TCP/IP is functioning properly on your system:

```
Ping 127.0.0.1
```



**REMEMBER** No matter what your IP address is, the loopback address is a constant that you can use to verify that your system is running correctly.

Here's an IP address example: Computer A has an IP address of 194.12.11.10, and it initiates communication with computer B, whose IP address is 194.13.11.9. Are the two workstations on the same network? Looking at the first octet, you can see that the number 194 is a Class C address, which means that the first three octets make up the network ID, and the last octet is the host ID. Because there is a difference in the first three octets (which is the network ID), these two computers are on different networks.



**TIP** Identifying whether the computer you are trying to communicate with is on your network could be important when troubleshooting communications. If the computer you are trying to communicate with is not on your network, the problem could be with your computer, the remote computer, or the router. This means you have more places to look for the cause of the problem.

## ***Subnet mask versus CIDR***

Another way to tell whether your computer is on the same network as the computer you are trying to communicate with is to look at the subnet mask. The *subnet mask* is what your computer uses to determine whether the network device it is trying to communicate with is on the same network. The subnet mask helps the system determine the network ID portion of the IP address by comparing the subnet mask against the IP address. If there is

a 255 in the subnet mask, the corresponding octet in the IP address is part of the network ID. After the network ID is known, any systems that have the same network ID are considered to be on the same network; otherwise, they would have a different network ID.

Different classes of IP addresses are associated with different default subnet masks. For example, a Class A address has a default subnet mask of 255.0.0.0, a Class B address has a default subnet mask of 255.255.0.0, and a Class C address has a default subnet mask of 255.255.255.0.

Looking at the subnet masks, any octet with the value of 255 means that the corresponding octet in the IP address is part of the network ID.

To put this all together, [Table 3-2](#) shows an example of two computers and their IP address configurations.

**TABLE 3-2 Comparing IP Addresses with Subnet Mask**

<i>Item</i>	<i>Address</i>
Computer A (IP address)	13.10.12.120
Computer A (subnet mask)	255.0.0.0
Computer B (IP address)	18.23.48.119

Using this example, computer A tries to connect to computer B. The first thing that computer A does is compare its IP address with its own subnet mask to determine what octets make up the network ID. Here it sees that the first octet is the network ID because the subnet mask has the number 255 in only the first octet. Then computer A compares its subnet mask with the IP address of computer B (the remote computer it is trying to communicate with) and identifies that the network IDs of computer A and computer B are different — the two computers are on different networks.

When computer A realizes that the remote computer it is trying to communicate with (computer B) is on a different network, it starts to panic because it doesn't have the capability to send the information to the other computer. Computers can pass information directly to other

computers only if both systems are on the same network. So what happens? This is where the default gateway fits into the story.

Before moving on to the default gateway, I first want to talk about CIDR notation. It is common for IT professionals to document an IP address, but instead of specifying the subnet mask, they use CIDR notation to specify it instead. With CIDR notation, the number of bits in the subnet masks that have been enabled (set to a 1 state) are specified. For example, a subnet mask of 255.0.0.0 has the first 8 bits enabled (set to 1), while the last 24 bits are set to 0. This means the CIDR notation is /8. To document a class A IP address that has a subnet mask of 255.0.0.0 using CIDR notation would be something like this: 24.56.7.22/8. Class B addresses have a CIDR notation of /16 (subnet mask of 255.255.0.0), and class C addresses have a CIDR notation of /24 (subnet mask of 255.255.255.0).

## *Default gateway*

When information has to be forwarded from a computer on one network to a computer on another network, a special network device called a *router* must be used. The router has a table that lists all the networks it knows about and the network ID associated with each of those networks. When the router receives information destined for a particular IP address, it checks its table of network IDs for a match. If a match is found, it delivers the information to the appropriate network.

How does the information get to the router so that it can be forwarded? Looking at the example from [Table 3-2](#) in the previous section, computer A has information for computer B, and computer A realizes that computer B sits on a different network. At this point, computer A looks at its *default gateway*, which is the address of the router that will forward the information on to computer B's network. Note that the address of the default gateway must use the same network ID as the local system. The default gateway is a TCP/IP option configured on each workstation. Typically, all computers on the same network point to the same router.

When you are comfortable with the concepts of an IP address, subnet mask, and default gateway, you are ready to configure these options on a Windows OS, which I cover in the next section.

## *Configuring TCP/IP in Windows*

There are a number of ways IP address configuration settings can be assigned to your systems and devices. The following is a quick summary of these common techniques to assign IP address information:

- » **Static:** Static configuration means you must manually enter the IP address, subnet mask, default gateway, and other TCP/IP settings that are required, such as DNS.
- » **Dynamic:** Dynamic configuration means that a system or device automatically receives the IP address information assigned from a DHCP server.
- » **APIPA:** If you have your device configured to obtain an IP address automatically (which means from DHCP), and there is no DHCP server available, your system will assign itself an IP address in the 169.254.x.y address range. This is known as Automatic Private IP Address and is an IPv4 feature.
- » **Link local:** Similar to IPv4 having the APIPA feature, IPv6 has the link local feature. A link local address is an IPv6 address that is automatically configured and allows the host to access the local network.

Let's take a look at static and dynamic configuration in a bit more detail.

### *Static configuration*

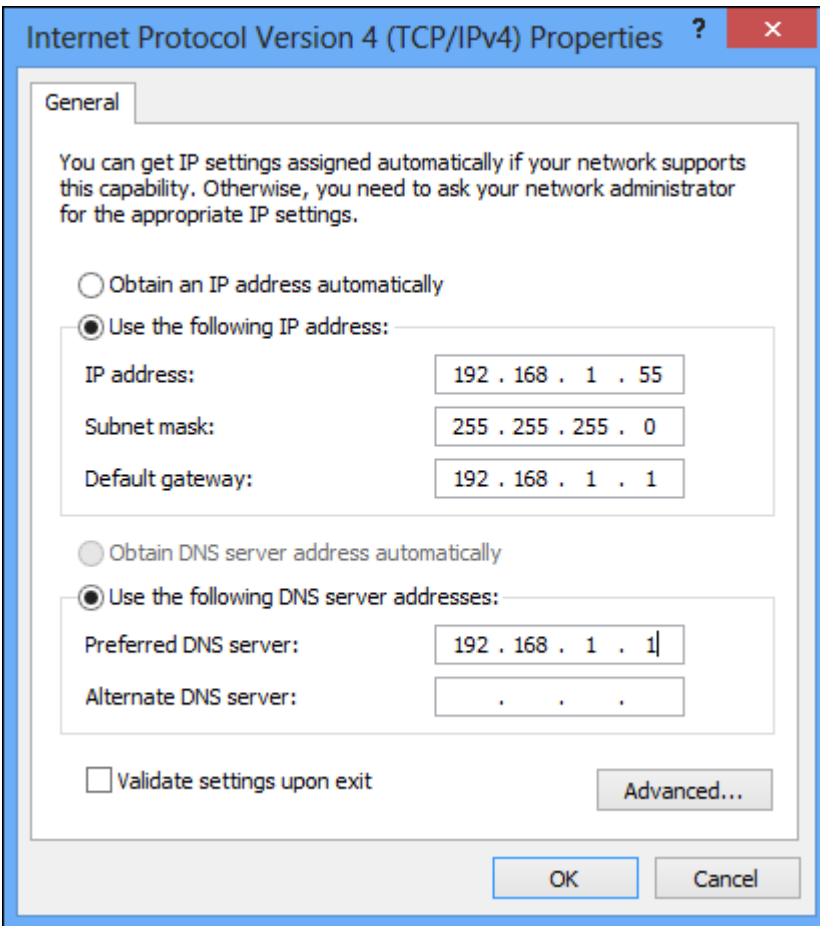
To configure TCP/IP on a Windows system, access your local area connection properties and configure the TCP/IP protocol. Be aware that all Microsoft OSes today have TCP/IP installed by default. You simply need to configure the IP address on the system. To configure TCP/IP with static addresses on a Windows system, follow these steps:

#### **1. Locate the network connections:**

- *Windows 10:* Click the Start button, then type **control**. Choose Control Panel from under the Best Match section. Choose Network and Internet ⇒ Network and Sharing Center ⇒ Change Adapter Settings.

- *Windows 8*: Right-click the Start icon and then choose Control Panel ⇒ Network and Internet ⇒ Network and Sharing Center ⇒ Change Adapter Settings.
  - *Windows 7/Vista*: Click Start ⇒ Control Panel ⇒ Network and Internet ⇒ Network and Sharing Center, and then click the Change Adapter Settings link on the left.
2. **Right-click your network connection, which appears as local area connection (Windows 7) or Ethernet (Windows 8.1/Windows 10), and then choose Properties.**
  3. **Select Internet Protocol Version 4 (TCP/IPv4) and then choose Properties.**
  4. **To assign a static address, select Use the Following IP Address (as shown in [Figure 3-5](#)) and then type your computer's IP address, subnet mask, and default gateway in the corresponding text boxes.**
  5. **Type the address of your DNS server in the Preferred DNS Server text box.**

To know what to enter as the IP address of your DNS server, consult the network administrator or maybe even the network architects. Whoever has designed the network knows the IP address of the DNS server. (DNS is covered in more detail in the section "[DNS](#)," later in this chapter.)
  6. **Click OK and then OK again.**



**FIGURE 3-5:** Configuring TCP/IP on a Windows client.



**FOR THE  
EXAM**

To communicate with systems off the network, your computer will need an IP address, a subnet mask, and a default gateway configured. To communicate with systems on the network, you need only an IP address and subnet mask configured.

### ***Configuring TCP/IP en masse using DHCP***

If you are the network administrator of a large network, you do not want to run around to 400 workstations and configure an IP address, a subnet mask, and a default gateway on each computer. Not only is this time-consuming to initially set up, but it also becomes a nightmare to manage because of all the potential for human error. I have spent my days running around to each computer on the network, a sheet of paper in my hands,

making sure that each computer is configured properly, and I can tell you that it is *not* fun!

Today's network OSes support Dynamic Host Configuration Protocol (DHCP), which is a standard that allows the network administrator to tell the DHCP server a range of IP addresses that it is allowed to give out, along with the other TCP/IP options such as a subnet mask and default gateway. When the DHCP server is configured to give out the addresses, the desktop computers automatically request an IP address from the server when they start up, and the server hands them all the IP address information. This means that the network administrator does not have to run around to each computer individually to configure TCP/IP — which, in the long run, saves time and money.

The steps to configure a Windows system to obtain an IP address from a DHCP server are very similar to actually assigning the IP address manually.

To configure a Windows client for DHCP, follow these steps:

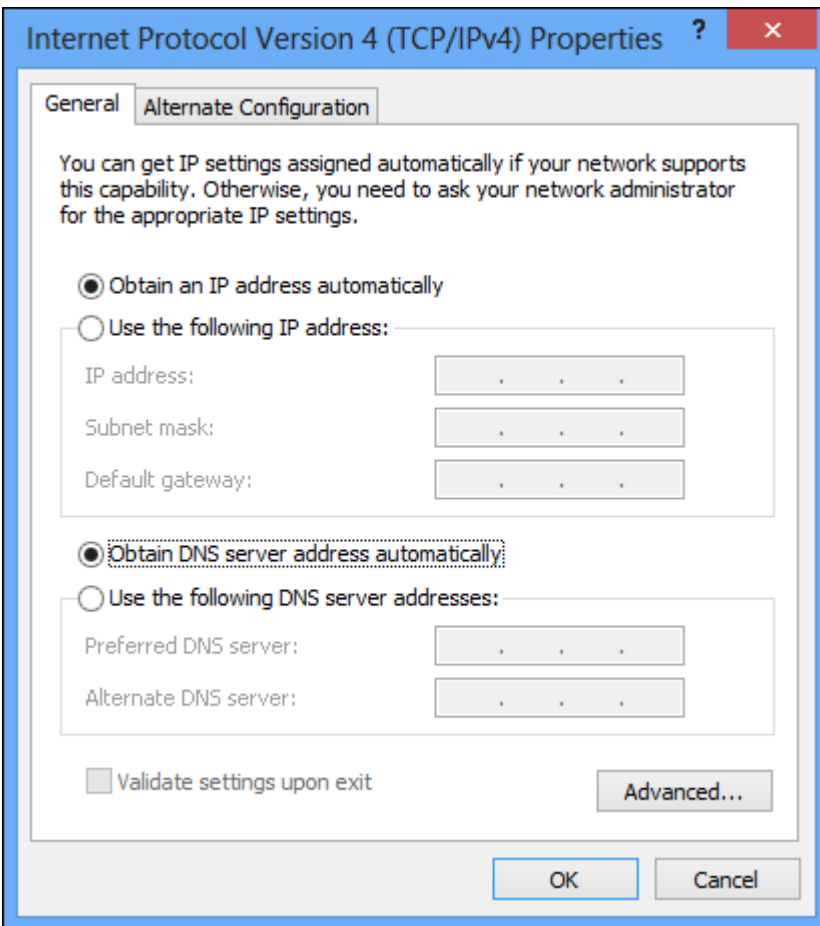
**1. Locate the network connections:**

- *Windows 10:* Click the Start button, then type **control**. Choose Control Panel from under the Best Match section. Choose Network and Internet ⇒ Network and Sharing Center ⇒ Change Adapter Settings.
- *Windows 8.1:* Right-click the Start icon and then choose Control Panel ⇒ Network and Internet ⇒ Network and Sharing Center ⇒ Change Adapter Settings.
- *Windows 7/Vista:* Click Start ⇒ Control Panel ⇒ Network and Internet ⇒ Network and Sharing Center, and then click the Change Adapter Settings link on the left.

**2. Right-click your network connection, which appears as local area connection (Windows 7) or Ethernet (Windows 8.1/Windows 10), and then choose Properties.**

**3. Select Internet Protocol Version 4 (TCP/IPv4) and then choose Properties.**

4. On the General tab, select the Obtain an IP Address Automatically option, as shown in [Figure 3-6](#), to enable this system to be a DHCP client.
5. Click OK and then OK again to close the network connections dialog box.



**FIGURE 3-6:** Configuring Windows as a DHCP client.

### *Alternate IP address*

When configuring your system to use DHCP, you will notice an Alternate Configuration tab within your TCP/IP settings (see [Figure 3-6](#)). The alternate IP address is a setting that allows you to assign a static IP address that you want the Windows system to use in case a DHCP server is not available to give an IP address to the client. From here you can configure an alternate IP address, subnet mask, DNS server, and default



gateway setting so that if your system is not able to obtain an IP address it will use the alternate address information.

Here's an example of where you can use the alternate IP address: If you are connecting a laptop at work, the laptop receives an IP address from the company DHCP server, but when you use the laptop at home, you may not have a DHCP server available. In that case, you can configure the system with an alternate address. If you do not configure the system for an alternate address and no DHCP server is available, you will receive an APIPA address. To learn more about APIPA addresses, read about special addresses next.

### *Reservations*

Reservations is a DHCP server configuration setting that allows you to specify on the DHCP server which IP address is assigned to which MAC address. It is a common feature used on networks so that administrators know which IP address is assigned to special systems or devices on the network. For example, if I wanted to ensure my laptop always had the same IP address even though I am using DHCP, I could find out the MAC address of my laptop (with `ipconfig/all`) and then configure a reservation on the DHCP server that specifies a certain IP address is to always be given to the system with that specific MAC address.

### *Special addresses*

When looking at IP addresses, you need to be familiar with a few special addresses when troubleshooting systems and preparing for your A+ certification exams!

#### *Loopback address*

The first special address to always remember is the loopback address. The loopback address is any address that begins with 127. Most IT professionals know the loopback address as 127.0.0.1, but it is really any address that starts with 127.

The loopback address is used to verify that the TCP/IP software is running fine on your system. In order to verify that TCP/IP is installed and running on your system, you can ping the address of 127.0.0.1. If you get

a reply, TCP/IP is running fine on your system. Otherwise, you need to re-install TCP/IP.

### ***Public addresses***

Most of the IP address ranges that exist are known as public addresses, which means that if your system is using one of the IP addresses, it is allowed to access the Internet using that address.

A few addresses are not considered public addresses, but are known as private addresses.

### ***Private IP addresses***

A private IP address is a type of IP address that is designed for local network communication only, and not for surfing the Internet. As mentioned, these addresses can be used to network machines on your LAN but cannot be used to surf the Internet because the addresses are for private use only.

The three private IP address ranges are

- » 10.0.0.0 to 10.255.255.255
- » 172.16.0.0 to 172.31.255.255
- » 192.168.0.0 to 192.168.255.255



**TECHNICAL  
STUFF**

It is interesting to note that the third range of 192.168.0.0 to 192.168.255.255 is what most home networks use because the home router is using that network range. I say this is interesting because you can surf the Internet at home using this address, but yet I say that private addresses cannot be used for Internet access. Huh? This doesn't make sense! To surf the Internet using a private IP address, you use a technology called Network Address Translation (NAT) that is built into the home router. More on NAT later in this chapter!

### ***Automatic Private IP Addressing (APIPA)***

As mentioned earlier in the chapter, if a DHCP server isn't available and your Windows clients are configured to obtain an IP address automatically, they will still receive an IP address because Windows operating systems support the Automatic Private IP Addressing (APIPA) feature. APIPA allows the client to self-assign an IP address if the DHCP server does not respond to the DHCP request. The address that the client self-assigns is within the 169.254.x.y network range. The system will also configure itself with a subnet mask of 255.255.0.0 but will not configure the default gateway entry. This means that if the DHCP server is down and your network clients boot up, they will all have an address in the 169.254.x.y range and will be able to communicate with one another. Because they are not configured for a default gateway entry, they will not be able to communicate with systems off the network or with the Internet.



**FOR THE  
EXAM**

When troubleshooting networking connectivity, use the `ipconfig` command to view the TCP/IP settings on a client. If the IP address is 169.254.x.y, that means the client cannot communicate with the DHCP server. Make sure that the client is connected to the network correctly and then verify that the DHCP server is functioning!

## ***Network Address Translation***

Home routers use the Network Address Translation (NAT) technology. The router is a NAT device, and a NAT device has two network cards: one connected to the Internet and one connected to the inside network. Your client systems use the NAT device (the home router) as their default gateway, so they send all outbound Internet traffic to the NAT device.

The NAT device converts the private address being used as the source IP address of the packet to the public address assigned to the WAN interface on the NAT device. As a result, the packet looks like it is coming from the WAN port of the NAT device, which is actually using a valid public address. When the reply comes back, the NAT device translates the address back to the private address and then sends the packet to the client

system inside the network. This is completely transparent to the clients on the network.

One benefit of NAT is that you can share the one public IP address assigned by your ISP to the WAN port on the router, thus allowing you to have multiple computers on your home network surfing at the same time. Another benefit is a security benefit: That is, your internal network structure is hidden from the outside world. From the Internet's point of view, the system surfing the web is the NAT router. If nefarious folks decide to attack that address, they are attacking the NAT device — and not the IP of a machine on your network.

## ***Proxy settings***

Some companies use what is called a *proxy server*, which implements NAT along with the capabilities to authenticate the individual trying to surf the Internet and authorize the website they are trying to access. Proxy servers are a great way for companies to monitor Internet usage and control what protocols and sites users can visit. For example, if the company decides that employees are spending too much time on websites such as Facebook during work hours, the company can have the proxy administrator disable access to that site.

In order to block access to websites, the company has to configure the employee's web browser to navigate through the proxy server to get to the Internet. The following steps show how to configure Internet Explorer on a Windows system to use a proxy server:

- 1. Launch Internet Explorer with the quick launch button in the Taskbar.**

If you don't see Internet Explorer in the Taskbar, you can find it in the Start menu.

- 2. Once you are in Internet Explorer, click the Tools button (gear icon in the top-right corner) and choose Internet Options.**

- 3. Click the Connections tab.**

- 4. At the bottom of the screen in the Local Area Network (LAN) Settings area, click the LAN Settings button.**

5. At the bottom of the dialog box, in the Proxy Server section, select the Use a Proxy Server for Your LAN check box.
6. Type the IP address of the proxy server in the Address field.
7. Click OK, and click OK again to exit.

## *IPv4 versus IPv6*

All the IP address information you have read about in this chapter is in regard to IP version 4 (IPv4). You now know that IPv4 addresses are 32-bit values that take a dotted-decimal notation such as 192.168.1.33.

Two major flaws exist with IPv4:

- » **Running out of IP addresses:** Partly because only 32 bits are in an IPv4 address and because of the growth of the Internet, we are running out of IP addresses.
- » **No security:** IPv4 was designed to allow communication and was not focused on making sure that communication was secure.

With the IPv6 protocol, the IP addresses are 128 bits long in hopes that we will never run out of addresses. The entire format for the IP addresses was also changed in IPv6. The addresses are now in hex values and look similar to the following address:

```
fe80:0000:042b:9853:1ff2:4cd3:2ff3:5cd2
```

The IPv6 protocol is designed with security in mind, and security protocols are built right into IPv6 itself. For example, IPv6 has IPSec capabilities, which allow traffic to be encrypted.

## *VLANs*

Virtual LANs (VLANs) are a hot topic today as they give us great flexibility as network administrators. Before VLANs, if you wanted to have two networks, let's say an accounting network and a marketing network, you had to purchase two different switches and not connect them together. This way you ensured there were separate networks for each of

those departments. With VLANs, you can purchase one switch (the switch must support VLANs), and then configure the switch with two different virtual LANs — one for accounting and one for marketing. You then specify which ports of the switch are part of each VLAN. By default, systems connected to ports on one VLAN cannot communicate with systems on the other VLAN unless you configure routing between the VLANs.

VLANs are a big security feature as they allow you to restrict communication between different types of systems.

The reason I mention VLANs in this chapter is because when it comes to IP address assignment, each VLAN will need its own network ID (range of addresses). For example, if you divided your switch into two VLANs, then you will need two IP ranges such as 192.168.1.0 (accounting network) and 192.168.2.0 (marketing network).



**FOR THE  
EXAM**

For the A+ exam, remember that VLANs are used to break the network into multiple subnetworks. Also remember that each VLAN will need its own network ID when IP addresses are being assigned.

## *Understanding Name Resolution*

To communicate with another computer across a TCP/IP network, you have to know the IP address of the computer you are trying to communicate with. This is unrealistic, considering that you are probably not too interested in trying to memorize all the IP addresses of the different websites you visit every day.

When running a TCP/IP network, you assign a friendly name to each computer and reference each computer by the friendly name instead of using the IP address. This means that instead of using an address like 204.56.78.6 to connect to Bob's computer, you would use a friendly name — say, bob.

The two types of names to understand when troubleshooting TCP/IP networks are

- » Computer names (also known as *NetBIOS names*)
- » Fully qualified domain names (FQDNs)

## *NetBIOS names*

In the Windows world, you access resources on a system by connecting to the computer name of the system. As an administrator, you assign a computer name to each computer on the network. The *computer name* (NetBIOS name) is a friendly name of as many as 15 characters assigned to a computer and used to uniquely identify the computer on the network. Users can then connect to the computer by the computer name *or* by the IP address — and people find it much easier to remember the computer name!

## *Changing the computer name in Windows*

Changing your computer name in Windows is a common task, and is fairly straightforward with today's Windows OSes.

To change your computer name in Windows, follow these steps:

1. **Navigate to Control Panel:**
  - a. **Choose Start ⇒ Control Panel (in Windows 7) or right-click the Start icon in Windows 8.1, and then choose Control Panel.**
  - b. **In Windows 10, click the Start button and type control. Choose Control Panel from the Best Match section.**
2. **In the Control Panel, choose System and Security and then choose System.**

You can see the computer name toward the bottom of the screen.
3. **To change the computer name, click the Change Settings link that appears on the right next to the computer name.**
4. **Click the Change button.**

The Computer Name Changes dialog box appears, allowing you to type a new computer name, as shown in [Figure 3-7](#).



**TIP**

When changing your computer name, notice that you can set the workgroup as well. A *workgroup* is the term given to a logical grouping of computers. When users browse the network, they may choose a workgroup, such as Accounting, and then they will see any systems that are a part of the Accounting workgroup. To place your system in a particular workgroup, simply type the name of the workgroup in the text box.

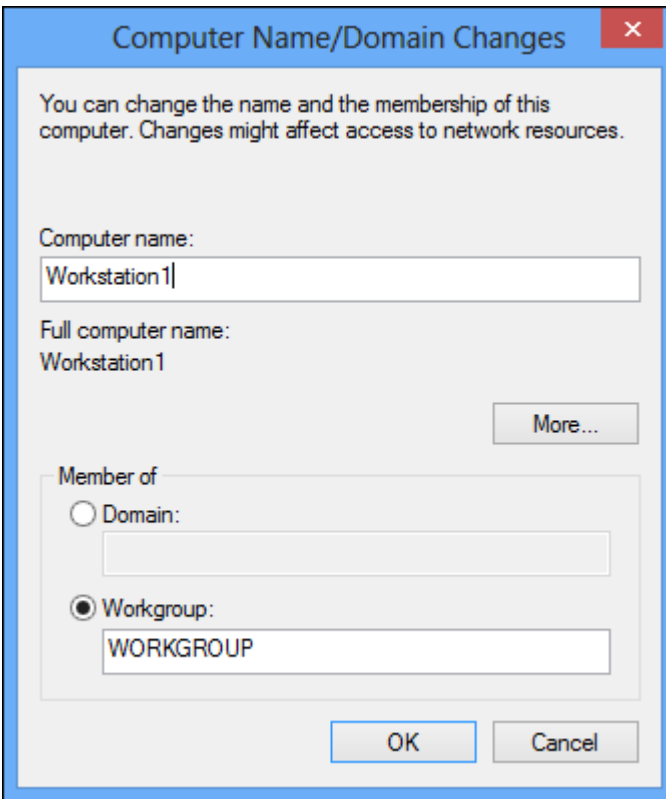
5. **Type a new computer name and workgroup for your system and then choose OK to close out all the dialog boxes.**
6. **Reboot the system.**



**TIP**

The computer name does not take effect until you reboot the system.





**FIGURE 3-7:** Changing your computer name in Windows.

## ***WINS***

When you network in a Microsoft environment, you connect to other computers by using those computers' names. These computer names must be converted to IP addresses for communication to happen in a TCP/IP network. For example, you may want to connect to Bob's computer, so you connect to `\\bob` through the `Run` command on the Start menu. When you try to connect, `\\bob` has to be converted to an IP address for the computer to be able to look for it. The process of converting a name from one format to another is *name resolution*. In this example, the computer name is being converted to an IP address, which is known as *NetBIOS name resolution*.

With NetBIOS name resolution, before your computer tries to connect to another system, it sends a query to a Windows Internet Naming System (WINS) server, asking the server this: "Hi there, Mr. WINS server. I am trying to connect to a computer named `bob` — do you have an IP address for this computer?" The WINS server holds a database of NetBIOS names

and matching IP addresses: the WINS database. Think of this database as having two columns: one for the computer name (NetBIOS name) and one for the matching IP address. Upon receiving the question, the WINS server checks the database for the computer named `bob` and then returns its IP address to the client who asked for it. Then the client can connect by using the IP address for `bob`.

For a Windows system to send a query to the WINS server, you must ensure that you configure the WINS server setting within the TCP/IP properties of the client system. Configuring the Windows client for a WINS server directs the client to the server that it must register its name and IP address with and also whom to send name resolution queries to.

Before configuring your clients for WINS, you must be aware of the IP address used by the WINS server. If you do not know this information, consult the network administrator. After you have the IP address of the WINS server, you are ready to configure the WINS clients. To configure a Windows system as a WINS client, follow these steps:

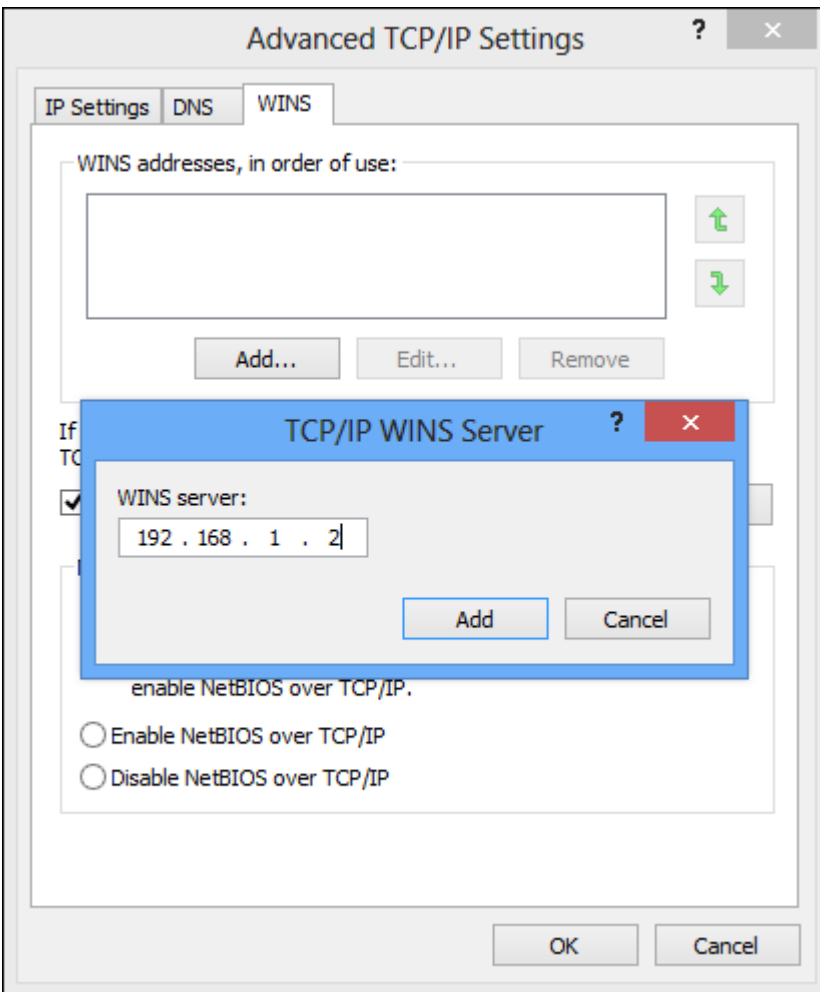
**1. Locate the network connections:**

- *Windows 10:* Click the Start button, then type **control**. Choose Control Panel from under the Best Match section. Choose Network and Internet ⇒ Network and Sharing Center ⇒ Change Adapter Settings.
- *Windows 8.1:* Right-click the Start icon and then choose Control Panel ⇒ Network and Internet ⇒ Network and Sharing Center ⇒ Change Adapter Settings.
- *Windows 7/Vista:* Click Start ⇒ Control Panel ⇒ Network and Internet ⇒ Network and Sharing Center and then click the Change Adapter Settings link on the left.

**2. Right-click your network connection, which appears as local area connection (Windows 7) or Ethernet (Windows 8.1), and then choose Properties.**

**3. Select Internet Protocol Version 4 (TCP/IPv4) and then choose Properties.**

4. In the Internet Protocol (TCP/IP) Properties window, click the **Advanced** button.
5. Click the **WINS** tab.
6. Click the **Add** button to add the IP address of the WINS server.
7. Type the IP address of the WINS server and click **Add**, as shown in [Figure 3-8](#).
8. Keep clicking **OK** until you close all dialog boxes.

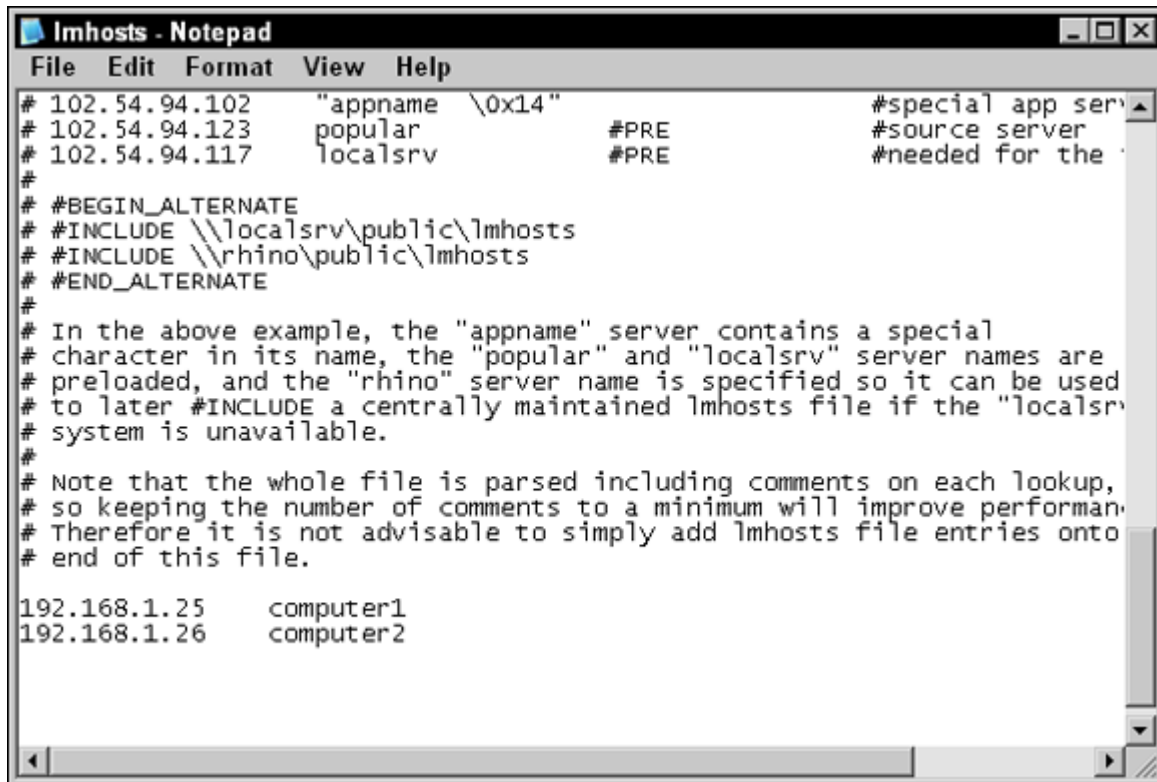


**FIGURE 3-8:** Configuring a WINS client in Windows.

### *The LMHOSTS file*

If you do not have a WINS server but an application you are running requires the use of a NetBIOS name (computer name), you need to use the `LMHOSTS` file. The `LMHOSTS` file resides on each computer and is used to

resolve, or convert, computer names to IP addresses. This file exists on each system on the network. You simply need to add an entry for the computer name and the corresponding IP address for each system that you want the file to resolve. [Figure 3-9](#) displays a typical LMHOSTS file.



```
File Edit Format View Help
# 102.54.94.102 "appname \0x14" #special app serv
# 102.54.94.123 popular #PRE #source server
# 102.54.94.117 localsrv #PRE #needed for the
#
# #BEGIN_ALTERNATE
# #INCLUDE \\localsrv\public\lmhosts
# #INCLUDE \\rhino\public\lmhosts
# #END_ALTERNATE
#
# In the above example, the "appname" server contains a special
# character in its name, the "popular" and "localsrv" server names are
# preloaded, and the "rhino" server name is specified so it can be used
# to later #INCLUDE a centrally maintained lmhosts file if the "localsrv
# system is unavailable.
#
# Note that the whole file is parsed including comments on each lookup,
# so keeping the number of comments to a minimum will improve performan
# Therefore it is not advisable to simply add lmhosts file entries onto
# end of this file.

192.168.1.25 computer1
192.168.1.26 computer2
```

**FIGURE 3-9:** An example of an LMHOSTS file in Windows.

Windows stores the file in %systemroot%\system32\drivers\etc. In Windows, the folder has an existing LMHOSTS file that you can use as a sample, but it has a .sam extension that needs to be removed because the true LMHOSTS file has no extension.

## ***Fully qualified domain names (FQDNs)***

The other type of name that can be assigned to the computer when you are running a TCP/IP network is a host name, or a *fully qualified domain name (FQDN)*. FQDNs are used when you run a TCP/IP-based or Internet-based application, such as FTP, email, or web browser applications. For example, to navigate to my website via your favorite web browser, you would type [www.glenecclarke.com](http://www.glenecclarke.com) — this is an

example of an FQDN. An FQDN is an Internet-style name that needs to be converted to an IP address for communication to occur.

The point is that when you use a computer name or an FQDN on a TCP/IP-based network, the names always need to be converted to the actual IP addresses. Again, converting names (either computer names or FQDNs) to IP addresses is *name resolution*.

There are a few techniques for FQDN resolution, and some are more popular than others. The following sections describe the name resolution techniques and their purposes.

## **DNS**

DNS (Domain Name System) is the desired name resolution technique for resolving (converting) fully qualified domain names to IP addresses. Remember that FQDNs are the names that are used with Internet-based applications, such as email and web browsers. DNS is like a big database of FQDNs and their matching IP addresses. Think of this database as having two columns — one for the FQDN and the other for the IP address.

When you are running Internet or TCP/IP applications and you type in a FQDN, your computer sends a query to the DNS database asking something like this: “I am trying to connect to [www.glenecclarke.com](http://www.glenecclarke.com). Do you have the IP address that matches this FQDN?” The database looks up the FQDN and returns the IP address to your computer, and your computer then connects to that IP address.

The big question is, where is the database stored? The database is stored on DNS servers. These servers hold the actual records and also where each client computer on your network sends its name queries.

To configure a Windows client to use a DNS server, you add the IP address of the DNS server while configuring TCP/IP. (Refer to the section “[Configuring TCP/IP in Windows](#),” earlier in this chapter.) Notice also that in Windows, the DNS server option is on the same screen as where you assign the IP address for a computer, which shows how critical DNS is to today's computing! To configure a Windows client to use DNS, follow these steps:

**1. Locate the network connections:**

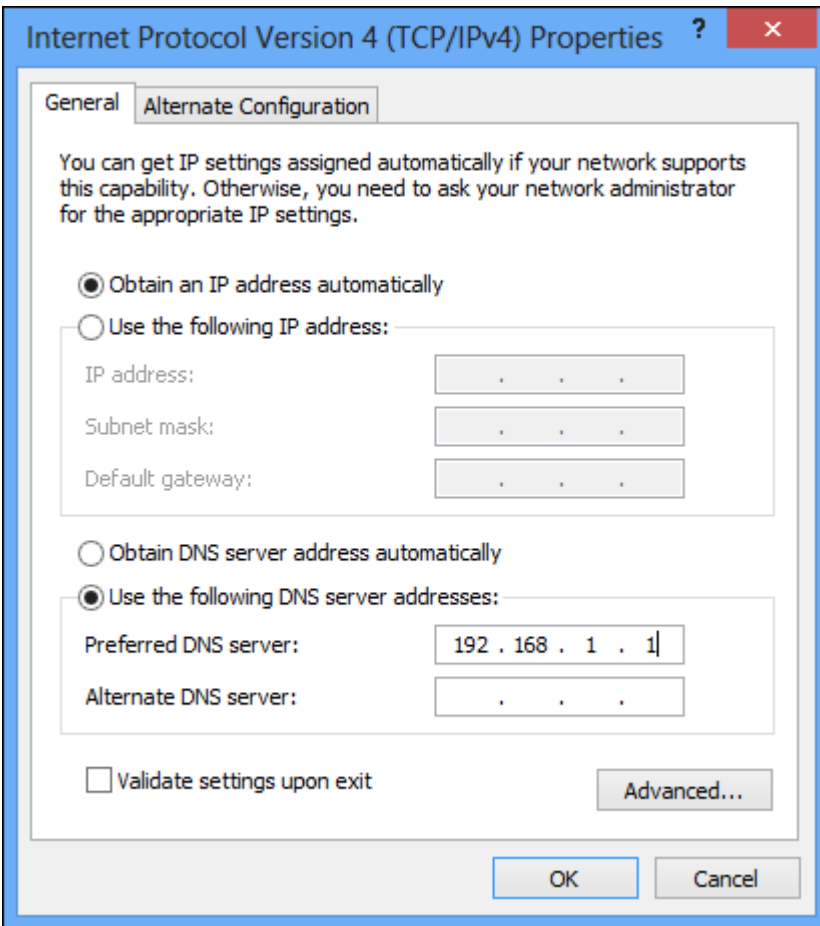
- *Windows 10:* Click the Start button, then type **control**. Choose Control Panel from under the Best Match section. Choose Network and Internet ⇒ Network and Sharing Center ⇒ Change Adapter Settings.
- *Windows 8.1:* Right-click the Start icon and then choose Control Panel ⇒ Network and Internet ⇒ Network and Sharing Center ⇒ Change Adapter Settings.
- *Windows 7/Vista:* Click Start ⇒ Control Panel ⇒ Network and Internet ⇒ Network and Sharing Center and then click the Change Adapter Settings link on the left.

**2. Right-click your network connection, which appears as local area connection (Windows 7) or Ethernet (Windows 8.1), and then choose Properties.**

**3. Select Internet Protocol Version 4 (TCP/IPv4) and then choose Properties.**

**4. In the TCP/IP Properties dialog box, select the Use the Following DNS Server Addresses option and type the IP address of your DNS server, as shown [Figure 3-10](#).**

**5. Click OK twice to close the dialog boxes.**

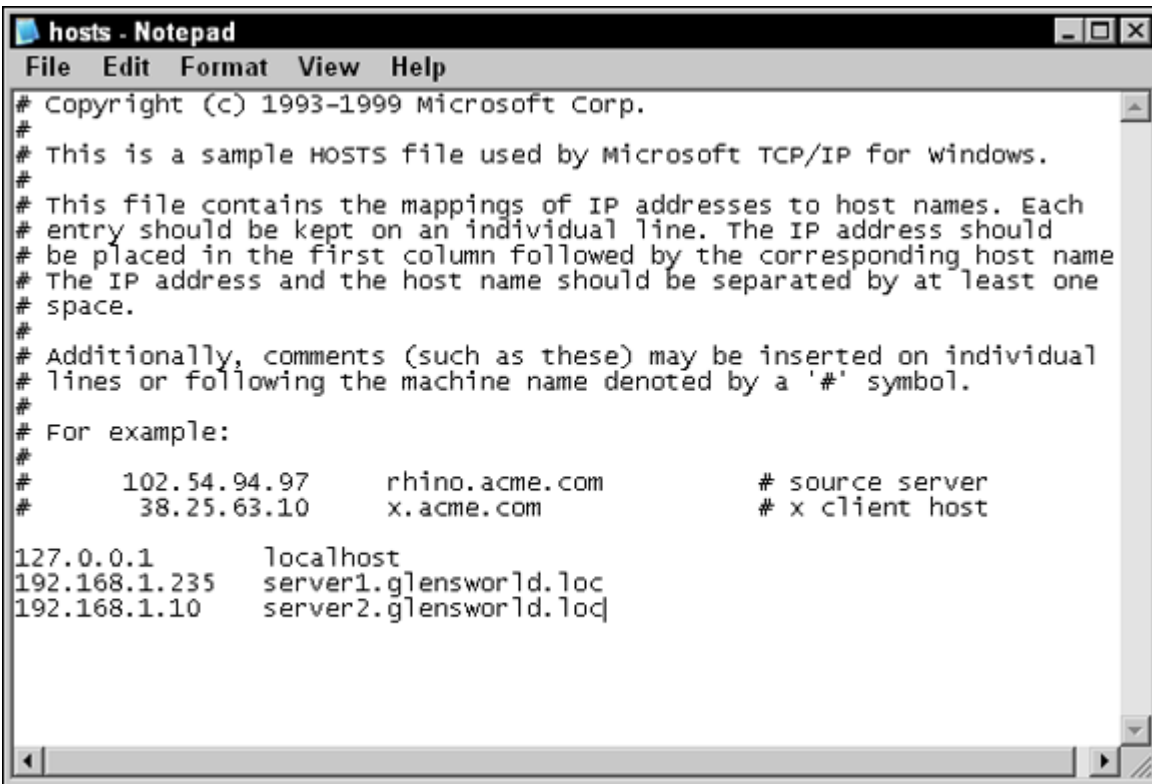


**FIGURE 3-10:** Configuring a Windows client for DNS.

### *The HOSTS file*

Very similar to the idea of using an `LMHOSTS` file for NetBIOS name resolution (see “[The LMHOSTS file](#)” section, earlier in the chapter), you can use a text file, called the `HOSTS` file, for host name resolution. The `HOSTS` file is located in the `%systemroot%\system32\drivers\etc` folder on Windows systems.

The configuration of the `HOSTS` file is similar to the configuration of the `LMHOSTS` file. You simply create two columns — one for the FQDN and the other for the IP address of the system. Separate these columns with a tab. [Figure 3-11](#) shows a sample `HOSTS` file.



```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com           # source server
#       38.25.63.10       x.acme.com               # x client host

127.0.0.1       localhost
192.168.1.235    server1.glensworld.loc
192.168.1.10     server2.glensworld.loc
```

**FIGURE 3-11:** An example of a `HOSTS` file used for FQDN resolution.

## ARP

Be aware that another layer of resolution needs to happen after your client has the IP address of the system it wants to communicate with. You know that there is a different database for FQDN resolution and computer name resolution: namely, the DNS database stores FQDNs and their IP addresses, and the WINS database stores computer names and associated IP addresses. After the name is converted to the IP address, the IP address then must be resolved to the hardware address burned into the network card. This hardware address assigned to each network card is the MAC address. This means that there has to be a process that converts the IP address to the MAC address, and this process is Address Resolution Protocol (ARP). ARP is an address resolution protocol that converts the IP address to the physical address assigned to the network card.

ARP is a broadcast, or a yell, out on the wire for a particular address. Look at an example of computer A trying to send information to computer B: After computer A has the IP address of computer B (204.56.78.3), computer A yells at the top of its lungs, “Hey, 204.56.78.3! What is your



network card's MAC address?” This yell runs along the network and eventually reaches computer B, which responds with its MAC address. After computer A has the MAC address of computer B, it can then send the data to computer B.



TECHNICAL  
STUFF

ARP messages are *broadcast messages*, and broadcast messages do not pass through routers. This does not cause a problem because when you want to communicate with a system on a different network, your system sends the data to the default gateway, or router, and then the router sends the data off the network by ARPing the router on the destination network. In this example, your system communicates with the router, so it would ARP the router, not the destination system!

## REAL-WORLD SCENARIO: PLANNING TCP/IP SETTINGS

Determine what TCP/IP services are required to fit the following scenario. The answer follows the scenario.

**Scenario:** You are responsible for implementing a TCP/IP-based network across all office locations in your region. What TCP/IP options will you set, and which additional TCP/IP-based services will you implement?

**Answer:** You might want to set a DNS server to store the FQDN and IP addresses of the different servers on your network. You might also want to run a WINS server for computer name resolution because it is a WAN environment.

After you set up the DNS and WINS servers, you will install a DHCP for each network segment so that you can hand out IP address, subnet mask, and default gateway information to the clients on the network. You will also hand out the IP address of the DNS server and the WINS server through DHCP so that the clients are fully configured.



FOR THE  
EXAM

DNS and the `HOSTS` file resolve FQDNs to IP addresses. WINS and the `LMHOSTS` file resolve computer names to IP addresses.

# *Looking at Protocols and Ports*

When you run networking applications on a computer, each of those applications runs on a unique port address. The port address is a number that data is sent to in order for it to reach the application. For example, if you are running a web server on a system, the web server software uses port 80, but the email server software uses a totally different port number — 25 (and Minecraft uses port 25565!). Ports are the reason why our systems can receive different types of network traffic and the computer does not confuse the types — email traffic is received on port 25, while web traffic is received on port 80.

## *TCP versus UDP*

Along with the port, you should understand that most network communication uses either the *Transmission Control Protocol (TCP)* or the *User Datagram Protocol (UDP)*. If a network application uses TCP, it is considered to be connection based — meaning that a system must introduce itself first to the other application and establish a connection before sending any data. Also TCP-based applications verify that any data sent is actually received by the other party; if not, the sending system will retransmit the data. A UDP-based application is considered connectionless because it does not establish a connection to another system and just sends the data off to the target system without any official introductions (connections). Also, UDP does not verify that the data reaches the destination like TCP does.

## *Common ports*

The A+ exams expect you to know the port numbers of common TCP/IP protocols:

- » **FTP:** The FTP protocol uses two ports: TCP port 21 as the control port, which carries the commands across the network to the remote system, and TCP port 20, which is used to transfer the data or files across the Internet.

- » **SSH:** The SSH protocol is used as a secure remote management protocol that runs on TCP port 22.
- » **Telnet:** Telnet uses TCP port 23 to perform remote management of a system with the communication unencrypted. Note that SSH is the secure replacement to Telnet.
- » **SMTP:** SMTP is the protocol of the Internet for sending email. SMTP uses TCP port 25.
- » **DNS:** DNS is used to resolve FQDNs to IP addresses. DNS uses UDP port 53 for DNS queries.
- » **HTTP:** Web pages are delivered to web browsers using the HTTP protocol, which uses TCP port 80.
- » **POP3:** The Internet protocol to read email is POP3, which uses TCP port 110.
- » **IMAP:** IMAP is a newer protocol for reading email that is designed to replace POP3. IMAP uses TCP port 143 and has more features than POP3, such as being able to filter what messages are downloaded to the client.
- » **HTTPS:** HTTPS is used to securely transmit web pages using TCP port 443.
- » **RDP:** The Remote Desktop Protocol (RDP) is used to carry screenshot information and keyboard input across the network when remotely managing a system. RDP uses TCP port 3389.
- » **NetBIOS/NetBT:** NetBIOS over TCP/IP is the use of NetBIOS names, such as computer name, and having that computer name used to connect to resources on a TCP/IP network. NetBT uses UDP ports 137-139.
- » **SMB/CIFS:** SMB is now known as CIFS and is the file sharing protocol within the Windows environment. SMB/CIFS runs on TCP port 445.
- » **SLP:** The service location protocol is a protocol that enables computers and devices on the network to locate a service without any previous configuration on the client. SLP uses UDP port 427.

- » **AFP:** The Apple Filing Protocol is a file sharing protocol for OS X and uses TCP port 548.
- » **DHCP:** DHCP delivers IP addresses to clients over UDP ports 67 and 68.
- » **LDAP:** LDAP is a directory access protocol, for example, to locate items in Active Directory that use TCP port 389.
- » **SNMP:** The Simple Network Management Protocol is used to manage a device on the network, or view running details of the device. It uses UDP 161 and 162.

You are also expected to know the purpose of some common TCP/IP protocols. The following list outlines TCP/IP protocols to know for the A+ exams:

- » **DHCP:** The Dynamic Host Configuration Protocol (DHCP) is a protocol that is designed to give IP addresses out to network devices.
- » **DNS:** The Domain Name System (DNS) is a name resolution protocol that converts fully qualified domain names (such as [www.glenecclarke.com](http://www.glenecclarke.com)) to IP addresses.
- » **LDAP:** The Lightweight Directory Access Protocol (LDAP) is the Internet protocol for accessing a directory service.
- » **SNMP:** The Simple Network Management Protocol (SNMP) is a protocol that allows you to remotely manage a device.
- » **SMB/CIFS:** The Server Message Blocks (SMB) protocol is the underlying protocol for allowing Microsoft systems to share network resources.
- » **SSH:** The Secure Shell (SSH) protocol is a secure replacement to the Telnet protocol. SSH can encrypt and authenticate network communications.
- » **AFP:** The Apple Filing Protocol is the file sharing protocol for OS X that allows Mac systems to share files with one another.
- » **NNTP:** The network news transfer protocol is used to transmit news articles between a news server and an NNTP news client.

- » **SFTP:** The Secure FTP (SFTP) protocol is the secure replacement to the FTP protocol and is used to secure communications related to file transfer.

## *Troubleshooting with TCP/IP Utilities*

After you have TCP/IP installed and configured and you have your TCP/IP network running, you need to be able to troubleshoot the network. When problems arise on a Windows network, you can use some of the following commands to do your troubleshooting:

- » `IPCONFIG/ifconfig`
- » `PING`
- » `TRACERT/traceroute`
- » `NBTSTAT`
- » `NETSTAT`
- » `PATHPING`
- » `NSLOOKUP`
- » `NET` commands

The following sections discuss these popular TCP/IP utilities that are used to troubleshoot TCP/IP connectivity.

### ***IPCONFIG/ifconfig***

On Windows systems, you can run the `ipconfig` (IP configuration) utility, which shows you the current TCP/IP configuration of the Windows desktop, such as the IP address, subnet mask, and default gateway. If the computer is a DHCP client, `ipconfig` identifies the server that has given the IP address and also shows how long the IP address will be used by the client. [Table 3-3](#) shows some of the switches supported by the utility `ipconfig.exe`.

## TABLE 3-3 IPCONFIG Switches

Switch	Description
/?	Shows a list of switches supported by <code>ipconfig.exe</code> and a brief description of each switch
/all	Shows all TCP/IP information — for example, DHCP lease period and the DNS server
/release	Releases the current IP address information assigned by the DHCP server
/renew	Requests new IP address information from the DHCP server
/displaydns	Displays the DNS resolver cache which stores recent results from DNS queries
/flushdns	Clears the DNS resolver cache

For example, to use the `ipconfig` utility and view just the basic TCP/IP settings, you type the following at a command prompt:

```
ipconfig
```

But to view all the TCP/IP settings, such as your MAC address or the IP address of your DNS server, DHCP server, and WINS server, use the `ipconfig/all` command. You might also view when your lease time is up for the address you have been assigned when you use the `/all` switch on `ipconfig`.

Before leaving the topic of viewing your IP address settings, I want to add the point that on a Linux system, you use the `ifconfig` command to view your TCP/IP settings.



ON THE  
WEB

Lab 3-1 gives you practice working with the `ipconfig` command. You can find Lab 3-1 on the companion website at [www.dummies.com/go/aplusaio](http://www.dummies.com/go/aplusaio).

## PING

One of the most popular TCP/IP utilities is the `ping.exe` utility. *Ping* (Packet Internet Groper) is used to test whether your computer can communicate with a remote network device. If the ping test is successful, you get a ping response from the remote device; if it is not successful, the response will time out. The general syntax for using the ping utility is `ping <IP address>`, the IP address being the IP address of the network device you are testing.

When troubleshooting TCP/IP communication problems, it is important to understand the steps to find exactly where the problem occurs. Is the problem in the computer you are using, in the computer you are trying to connect to, or in the default gateway?

[Table 3-4](#) lists the order in which to ping each network device when trying to figure out at what stage the TCP/IP communication is failing.

**TABLE 3-4 Troubleshooting Network Connectivity**

Address to Ping	Description
127.0.0.1	This IP address is the <i>loopback</i> address. It always tests your own workstation's TCP/IP software to ensure that it has loaded.
IP address of your computer	After you get a response from loopback, ping the IP address that has been physically assigned to your network card. To find out what IP address is assigned to your network card, use <code>ipconfig.exe</code> .
IP address of default gateway	If you get a response from your network card's IP address, ping the IP address of the default gateway. If you don't know the IP address of your default gateway, run <code>ipconfig.exe</code> to view the address of the default gateway. Remember that the default gateway is the router, which is responsible for passing information on to other networks. If you are having trouble communicating with the router, you can't communicate with any devices off the network.
IP address of remote computer	After verifying that the default gateway is not the problem, if you know the IP address of the computer you want to talk to (and chances are you don't because you are not the person who assigns the address to that computer), you can try pinging it. If you get a timeout at this step, you know that the computer you are trying to communicate with is the problem.



**REMEMBER** When you're troubleshooting a system that doesn't have Internet access, use the `ipconfig` utility to view the default gateway of the system; then ping the default gateway.

You also need to know that `ping -t` allows you to do a continuous ping, meaning that until you stop pinging with a Ctrl+C command (CTRL+C is a common keystroke in most OSes to stop a command), you will continue to ping the system indefinitely. Also know that if you want the ping utility to do name resolution, add `-a` to the command.



**ON THE  
WEB**

Lab 3-2 gives you practice changing your TCP/IP settings and working with the `ping` command. Lab 3-3 allows you to test your TCP/IP communication. Labs 3-2 and 3-3 can be found on the companion website at [www.dummies.com/go/aplusaio](http://www.dummies.com/go/aplusaio).

## ***TRACERT/traceroute***

The `ping` utility is probably the most used TCP/IP utility, and rightfully so. The `ping` utility is a very useful utility for troubleshooting communication problems, but the `ping` utility tells you only whether your computer has communicated with the remote hosts; it does not tell you what path the information took. This is where the *trace route* (`tracert.exe`) utility is useful. It is similar to the `ping` utility in the sense that responses are sent back to you if communication is established. The difference is that `tracert.exe` sends a response from every network it hits on the way, not just a response from the final destination. So `tracert.exe` shows you the *path* the information takes and also the number of networks between your computer and the computer you are talking to.

The trace route utility uses the following syntax (note the space after `tracert`):

```
tracert <IP address or DNS name>
```



It should be noted that to use `tracert` functionality on a Linux system, the command is `traceroute`, not `tracert`. Also remember that Linux is case-sensitive and as a result commands such as `traceroute`, `ping`, and `netstat` are in lowercase characters.

## NBTSTAT

Another popular network troubleshooting utility is `nbtstat`, which is used to troubleshoot NetBIOS name resolution. (Remember that discussion? If not, look back to the “[NetBIOS names](#)” section.) `nbtstat` stands for *NetBIOS over TCP/IP Statistics*. When your system resolves a computer name to an IP address, it stores that information in memory (the NetBIOS name cache) so that the next time the name needs to be converted to an IP address the request is resolved from cache instead of broadcasting or querying a WINS server. If you want to verify that the entry is in cache, use the `nbtstat` utility.

There are a number of uses for the `NBTSTAT` utility, so there are quite a few switches for the command. Some of the most useful switches are listed in [Table 3-5](#).

**TABLE 3-5 NBTSTAT Switches**

Switch	Description
/?	Shows a list of switches supported by <code>nbtstat</code> and a brief description of each switch.
-c	Displays the contents of the <code>NBTSTAT</code> cache. This cache shows the computer names and matching IP addresses that have been resolved recently.
-A <ip address>	Displays the list of NetBIOS names used by the IP address typed with the <code>-A</code> . The listing also indicates what types of services the system is running. Note that the <code>-A</code> is uppercase and has a space after it and before the IP address.
-n	Displays the NetBIOS names used by the local system.
-r	Lists which addresses have been resolved through WINS.

To use the `nbtstat` command, type something like the following at a command prompt:

```
nbtstat -A 192.168.1.200
```

## NETSTAT

The `netstat` command line utility (lowercase in Linux) is used to troubleshoot TCP/IP connections. If you use the `netstat` command by itself, it displays a list of connections that your system has with remote systems and the associated ports.

Like `nbtstat`, `netstat` supports a number of switches to help you get the most information possible out of the command. [Table 3-6](#) lists some of the more popular `netstat` switches.

**TABLE 3-6 NETSTAT Switches**

Switch	Description
/?	Shows a list of switches supported by <code>netstat</code> and a brief description of each switch.
-a	Displays all connections that your system has but also all listening ports. A port is what an application uses as an endpoint of communication. For example, applications such as Internet Explorer use a port, and that port is where a web server sends the data so that the data reaches Internet Explorer.
-o	Displays the process ID of the application that opened the port. You can use this information with the <code>tasklist</code> command to track down the application that opened the port. You can then use the <code>taskkill</code> command to terminate the program that opened the port.
-p <protocol>	Shows the connections for the protocol provided to the switch. For example, you could use <code>netstat -p TCP</code> to view all the TCP connections. In this example, you will not see the UDP connections.

An example usage of the `netstat` command is as follows:

```
netstat -a -o
```

## PATHPING

`pathping` is a newer command line utility to the Windows world that allows you to ping a destination, and — like the `tracert` command — you get a list of hops (routers) from the source to the destination. After the list of hops is determined, `pathping` sends a number of messages to each hop to calculate statistics on each hop, such as the number of lost packets.

## ***NSLOOKUP***

`nslookup` is a TCP/IP utility used to query DNS and to troubleshoot problems associated with DNS. With `nslookup`, you can query for a specific type of record, such as email server records (MX records) if you want to know the mail servers for a particular company. Take a look at a few `nslookup` commands.

```
nslookup www.glenecclarke.com
```

The preceding command queries DNS and reports back to you the IP address for the server at [www.glenecclarke.com](http://www.glenecclarke.com). To find the mail servers for `glenecclarke.com`, you would type the following commands in a command prompt:

```
nslookup  
set type=mx  
glenecclarke.com
```

In the previous example, Windows will report to you the entries from DNS that have an MX record type, which are the entries in DNS that reference the email servers for `glenecclarke.com`.

## ***NET commands***

Windows has a number of different networking commands that you can use to perform tasks such as create user account, modify group membership, and map network drives, to name a few.

### ***net user***

The `net user` command is used to view or manage user accounts on the system. When you go to a command prompt and type

```
net user
```

this command shows a list of user accounts that exist on the system. To create a user account, you can expand on the command by typing

```
net user aplusguy P@ssw0rd /add
```

This command creates a user named `apluguy` with a password of `P@ssw0rd`.

## *net localgroup*

The `net localgroup` command is used to manage membership to a specific group. If you want to add a user to the administrators group, you would type the following command:

```
net localgroup administrators aplusguy /add
```

## *net view*

You can also view a list of domains or workgroups on the network by using the `net view` command. The following shows a listing of domains:

```
net view /domain
```

From this list of domains, you can then view a list of servers in a particular domain by using the `net view` command as well. The following command is asking to view a list of systems in the `glensworld` domain:

```
net view /domain:glensworld
```

From the list of servers in the domain, you can then potentially view a list of shared folders on one of those systems by typing

```
net view \\server1
```

## *net use*

Don't confuse the `net user` command with the `net use` command. `net user` is used to manage user accounts, and `net use` is used to map network drives. For example, if you want to create a `J:` drive on your system that references the shared folder called `data` on a server called `Server1`, you would type

```
net use j: \\server1\data
```

These are just a few examples of popular networking tasks that can be performed by using the `net` commands in the Windows OS. To read more about what the `net` command can do in Windows, use the `net /?` command.

## *NETDOM*

Another common Windows command line tool that you can use is the `netdom` command. You can use `netdom` to perform a number of Active

Directory-related tasks such as join a computer to the domain, remove a computer from the domain, or reset the secure channel for computer accounts.

For example, to use `netdom` to join a computer to the domain, use the following command:

```
netdom.exe join %computername% /domain:DCATT /UserD:DCATT\administrator  
/PasswordD:Pa$$w0rd
```

In this case, the current computer is going to be joined to the DCATT domain using the administrator account.

## *Troubleshooting network issues*

Now that you understand some of the commands used to troubleshoot networking problems, I take a look at some common networking issues that arise from time to time.



**FOR THE  
EXAM**

The following are some common issues that you may need to troubleshoot; you definitely need to know these for the A+ exams:

- » **No connectivity:** If you have no connectivity to a network, you want to always check the physical connections first and then verify your network configuration, such as the IP configuration.
- » **APIPA address/link local address:** If you have an IP address of 169.254.x.y, you are having trouble obtaining an IP address from the DHCP server. You need to verify that the client is connected to the network properly and then check the DHCP server.
- » **Limited connectivity:** If you are connected to the network and experience limited connectivity, you should verify the IP settings such as the default gateway and the DNS server setting. Also verify that the router is connected to the Internet.
- » **Local connectivity:** If you experience local connectivity, only then double-check that the system has a default gateway configured and that the router has a connection to the Internet.

- » **Intermittent connectivity:** Intermittent connectivity issues are hard to troubleshoot. Verify that you do not have a problem with the cable, and check for devices that could be causing interference with your network (especially wireless networks).
- » **IP conflict:** If you have a duplicate IP address, you will not be able to network. Be sure that the IP address you are using is unique.
- » **Slow transfer speeds:** If you are experiencing slow transfer speeds, check the card settings and the settings on the router to see whether you can find a reason that the network devices would be using a slow transfer rate.
- » **Low RF signal:** If you have a low RF signal on a wireless network, you may need to go into the router and increase the power level of the signal.
- » **SSID not found:** If you are not able to locate the SSID for the wireless network you are trying to join, ensure that the wireless router is broadcasting the SSID.

## *Troubleshooting with hardware tools*

When troubleshooting network communication issues, you typically will find the problem is with logical issues, whether IP address configuration problems or name resolution problems such as DNS. Sometimes physical issues, such as cabling, are the cause of problems with the network. The following are some hardware tools that are often used to troubleshoot cabling issues:

- » **Cable tester:** A cable tester is a hardware device that is connected to both ends of the cable and is used to inform you if a signal can be sent from one end and received on the other. Cable testers are used to verify that the cable has been created, or crimped, properly.
- » **Loopback plug:** A loopback plug is a device that you can connect to communication equipment to ensure that the port on the communication equipment is working properly.

- » **Punchdown tool:** A punchdown tool, shown in [Figure 3-12](#), is used to connect the twisted pair cable to a patch panel or to secure the cable to the back of the wall jack.
- » **Tone generator and probe:** A tone generator and probe is used to locate a specific cable in a mess of cables.
- » **Wire strippers:** Wire strippers can be their own device or are part of the crimper, which is described next. Wire strippers are used to remove the outer shell of the cable to get access to the wire in the cable.
- » **Crimper:** A crimper, shown in [Figure 3-12](#), is a tool that is used to secure the connector to the end of the cable (for example, the RJ-45 connector to the end of the CAT 6 cable).
- » **Wireless locator:** A wireless locator is used to scan and identify wireless network and activity around you. This can be useful when troubleshooting wireless problems. Once a wireless network has been found, the wireless locator displays information about the wireless network such as the SSID, signal quality, MAC address, and the channel ID.



**FIGURE 3-12:** Punchdown tool (left) and crimper (right).

## *Sharing File System Resources*

In this section, I discuss how to set up the Windows OS for sharing network resources. I begin with a discussion of some of the core options that must be set to network within a Windows OS.

Every Windows computer must have a computer name to participate in a Windows network, and each computer name must be unique on the network to properly address a specific computer. To review the steps to change your computer's name, take a look at the section, “[Changing the computer name in Windows](#),” earlier in the chapter.

### *User-level access control*

Current versions of Windows operating systems use a type of access control known as user level access control. *User-level access control* means that when you share a resource out onto the network, you actually



assign permissions to particular users. If someone wants access to the share, his or her user account has to have been given permissions to the share, and the user must log in with that particular account.

## ***Enabling File and Printer Sharing in Windows***

Now that you understand the two levels of access control, you are ready to allow your Windows machines to share resources on the network. First, you must ensure that File and Printer Sharing Services are installed and that File and Printer Sharing is enabled. Then you can start sharing folders and printers.

All Windows OSes have File and Printer Sharing enabled by default. To verify that File and Printer Sharing is enabled within these operating systems, perform the following steps:

### **1. Locate the network connections:**

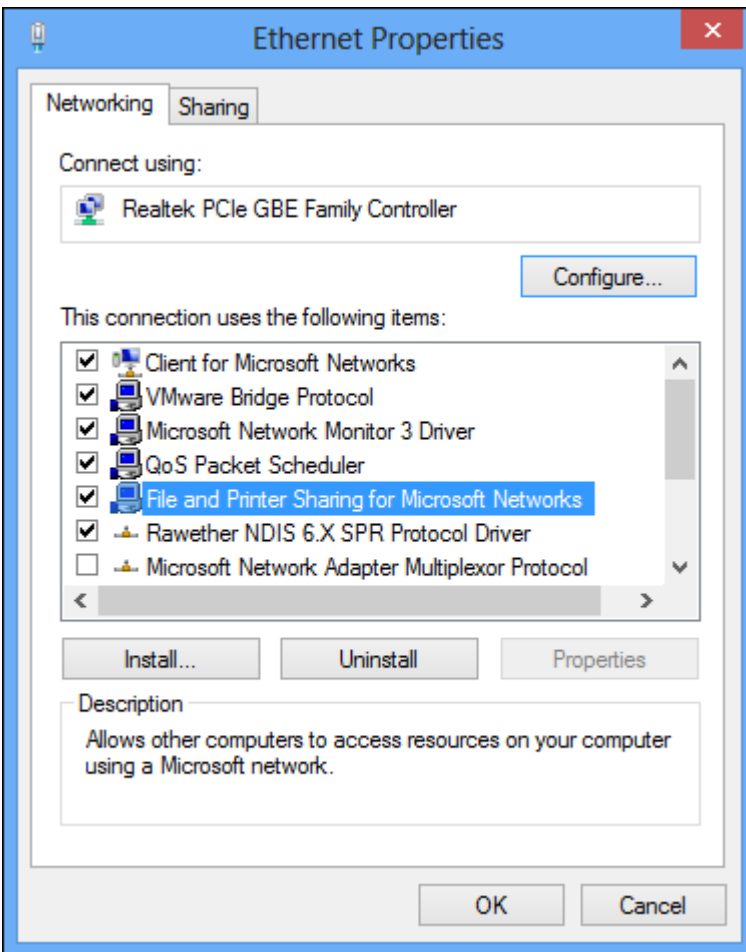
- *Windows 10:* Click the Start button, then type **control**. Choose Control Panel from under the Best Match section. Choose Network and Internet ⇒ Network and Sharing Center ⇒ Change Adapter Settings.
- *Windows 8.1:* Right-click the Start icon and then choose Control Panel ⇒ Network and Internet ⇒ Network and Sharing Center ⇒ Change Adapter Settings.
- *Windows 7/Vista:* Click Start ⇒ Control Panel ⇒ Network and Internet ⇒ Network and Sharing Center and then click the Change Adapter Settings link on the left.

### **2. Right-click your network connection, which appears as local area connection (Windows 7) or Ethernet (Windows 8.1), and then choose Properties.**

### **3. Select the File and Printer Sharing for Microsoft Networks check box, as shown in [Figure 3-13](#), and then click OK.**

When this check box is selected, File and Printer Sharing is enabled, and you're finished. If File and Printer Sharing for Microsoft Networks wasn't listed, you need to install it first, so keep reading.

4. If File and Printer Sharing isn't listed, click the Install button to install the service.
5. Choose Service in the Component Type dialog box and then choose File and Printer Sharing for Microsoft Networks. Then click OK to close all the dialog boxes.



**FIGURE 3-13:** Verifying that File and Printer Sharing is installed on Windows.

## *Creating shared folders*

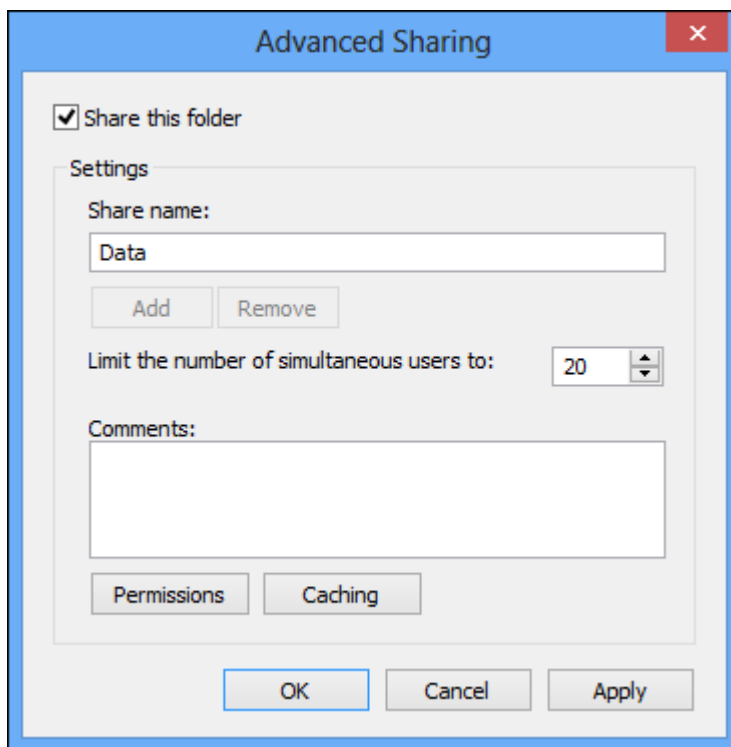
When a user on the network wants to access a file on another system, he must connect to a share on that system. *Shares* are a way to publish the folder on your system for other users on the network so that they can access the files in that folder. If you have not shared any resources, there is no reason for anyone to want to connect to your computer — it would be like giving someone the key to a locked but empty room.



**REMEMBER** You can share only folders or printers; you cannot actually share a file specifically. To allow users to access a file from across the network, you have to place the file in a folder and then share that folder.

### *Sharing a folder*

To share a folder on a Windows network, you typically must supply certain information such as the name of the share, permissions, and any caching settings you want (shown in [Figure 3-14](#)).



**FIGURE 3-14:** Sharing a folder.

Regardless of the version of the Windows operating system you are using, the following options are available when you share a folder:

- » **Share Name:** You need to give the share a name. This is the name that will be referred to by users who want to connect to the share.

- » **Comment:** This is an optional description of the share that displays in Windows when the user views the list of shares in Detail view.
- » **User Limit:** You may limit how many users can connect to the share at any given time. This could be useful if you notice that the system is slow after a certain number of users connect. For example, if you're sharing a CD-ROM, you may notice that access to the CD-ROM slows after six users connect. In this example, you may want to set the user limit to five. Setting the user limit to maximum allowed will configure the user limit for ten users connected to the share at once because Windows desktop OSes can allow only ten connections at a time.
- » **Permissions:** Set permissions on the share. You set permissions to control which users can modify data in the share and which ones can simply read information in the share.
- » **Caching:** This feature allows the client to store a local copy of data accessed in the share. This could be useful if you want to allow a laptop user to take a copy of the data home and update the data. The modified data could then be synchronized with the content on the server when the user returns to the office.

Notice in [Figure 3-14](#) that I shared the folder named Data. As mentioned earlier, when sharing a folder, you need to set the share permissions. To set the share permissions, click the Permissions button. The default permissions when sharing have changed over the last few versions of Windows. By default, everyone has the read permissions on shared folders.

When you share the folder, you should alter the default permissions to suit your needs. The following steps show you how to adjust these permissions to your liking:

1. **To remove the Everyone group from the permissions list, click the Remove button.**
2. **Add specific users to the permissions list by clicking the Add button.**

The Select Users or Groups dialog box appears.

**3. Select which user or group is allowed to connect to the share by selecting the user.**

You may add multiple users by clicking the first user, holding down the Ctrl key, and clicking additional users.

**4. Click Add to return to the Permissions dialog box.**

**5. To set a user's permissions, select one of the following permissions for that user:**

- *Full Control:* Allows a user to read and change the contents of files on the share, to delete files on the share, and to change the share permissions. This permission is not normally assigned to users.
- *Change:* Allows a user to read the contents of files in the share, change the contents of files that exist in the share, and delete files. Users cannot change permissions on the share with the Change permission.
- *Read:* Allows a user or group to read but not modify the content in the shared folder.

**6. Click OK and then click OK again to exit the dialog boxes.**

### ***Sharing a folder in Windows***

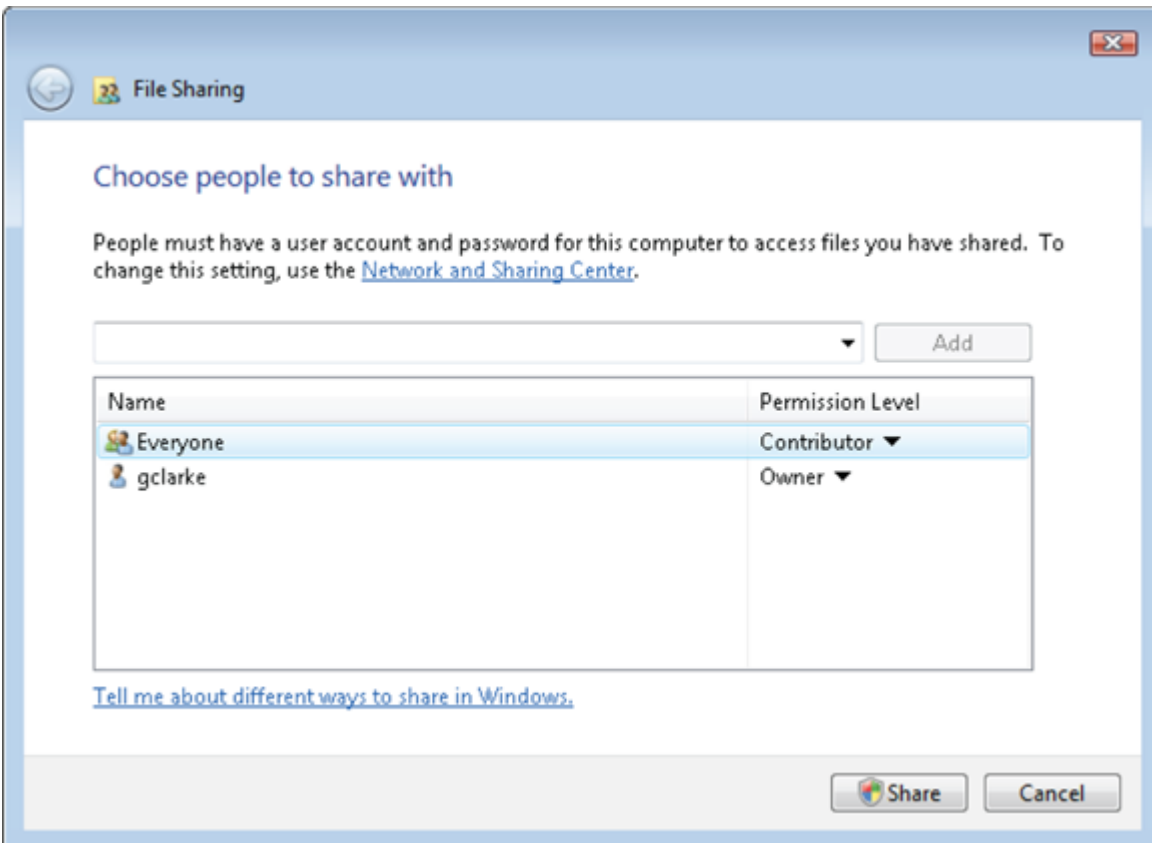
The steps to share a folder on a Windows 7, Windows Vista, or Windows 8.1 system are very similar. Microsoft has tried to simplify managing the security by creating a wizard-style interface to share folders. To share a folder in Windows, follow these steps:

- 1. Locate the folder you want to share on your system.**
- 2. Right-click the folder and choose Share With.**
- 3. In the File Sharing dialog box, choose the user (or group) you want to share the folder with from the drop-down list; then choose Add.**
- 4. Choose the Permission Level for the share (shown in [Figure 3-15](#)):**
  - *Reader:* Allows the user or group to read files from the share folder but not make changes to the content of the shared folder

- *Contributor*: Allows the user or group to add a file to the share and modify or delete his/her own files
- *Co-owner*: Gives the user full permission to the share, including modifying and deleting any files in the share.

5. Click the **Share** button.

6. Click **Done**.



**FIGURE 3-15:** Assigning permissions levels in Windows.

## *Hidden shares*

In the Windows world, you can also create hidden shares, which are like normal shares in the sense that users on the network can connect to them. The difference is that hidden shares are not advertised — you can't find them by browsing through the shared folder list on a server. Users will connect to the hidden share by typing the universal naming convention (UNC) in the `Run` command or by mapping a drive, which you can read about in the “[Connecting to shares](#)” section.

To create a hidden share, use the steps for creating a normal share (see the section “[Creating shared folders](#),” earlier in this chapter). However, when you type a share name in the Share Name text box, you create the hidden share by appending a dollar sign (\$) to the end of the share name. For example, if the share name is `data` and you want it to be a hidden share, you would type **data\$** in the Share Name text box. The share is then automatically hidden from Windows and users on the network when they browse the servers.

## *Multiple shares*

In Windows, you have the ability to create multiple shares for the same folder. This gives flexibility to the network administrator so that a user can have different permissions for a single folder, depending on what share that user connects to.



TECHNICAL  
STUFF

On my office network, I implemented multiple shares per shared folder so that during day-to-day activities, not even an administrator can alter files on the server. If an administrator wants to make changes to a folder, he has to connect to the secondary share for that particular folder to have full-control access. This helps prevent a lot of unfortunate mistakes in modifying or deleting files by accident — even network administrators make mistakes! A big rule I follow is “Protect the network from yourself as well!”

## *Connecting to shares*

After you create the shared resource, you can connect to the shared resource from anywhere on the network. There are a number of ways to connect to shared folders; here are a few of the most common:

- » Browsing network resources
- » Using a UNC path through the `Run` command
- » Mapping a drive through Windows or the `net` command

The following sections examine each of these methods.

### *Browsing network resources*

To browse network resources in Windows, follow these steps:

1. **Choose the File Explorer button in the Taskbar to browse files on the computer.**
2. **Expand Network on the left side of the screen in the folder listing.**  
You see a list of computers.
3. **Select a computer to see a list of shares on that computer.**
4. **You can open any share just by double-clicking it.**



**REMEMBER** You cannot see any hidden shares while browsing network resources. For this reason, it is important to know additional ways to connect to shares, such as through the UNC path.

To browse network resources in Windows Vista, you simply navigate to the network resources by choosing Start ⇒ Network. To view a list of shared resources on a system, double-click the system.

### *Using a UNC path*

You may also connect to a share by using the universal naming convention path. The UNC path is made up of two backslashes (\\), the computer name you want to connect to, one more backslash, and the share name of the folder you want to connect to. The entire syntax looks like this:

```
\\computername\sharename
```

You would type this into the `Run` command, found by clicking the Start button in Windows 7, or on a Windows 8.1 system, you simply type the UNC path while on the Start screen.





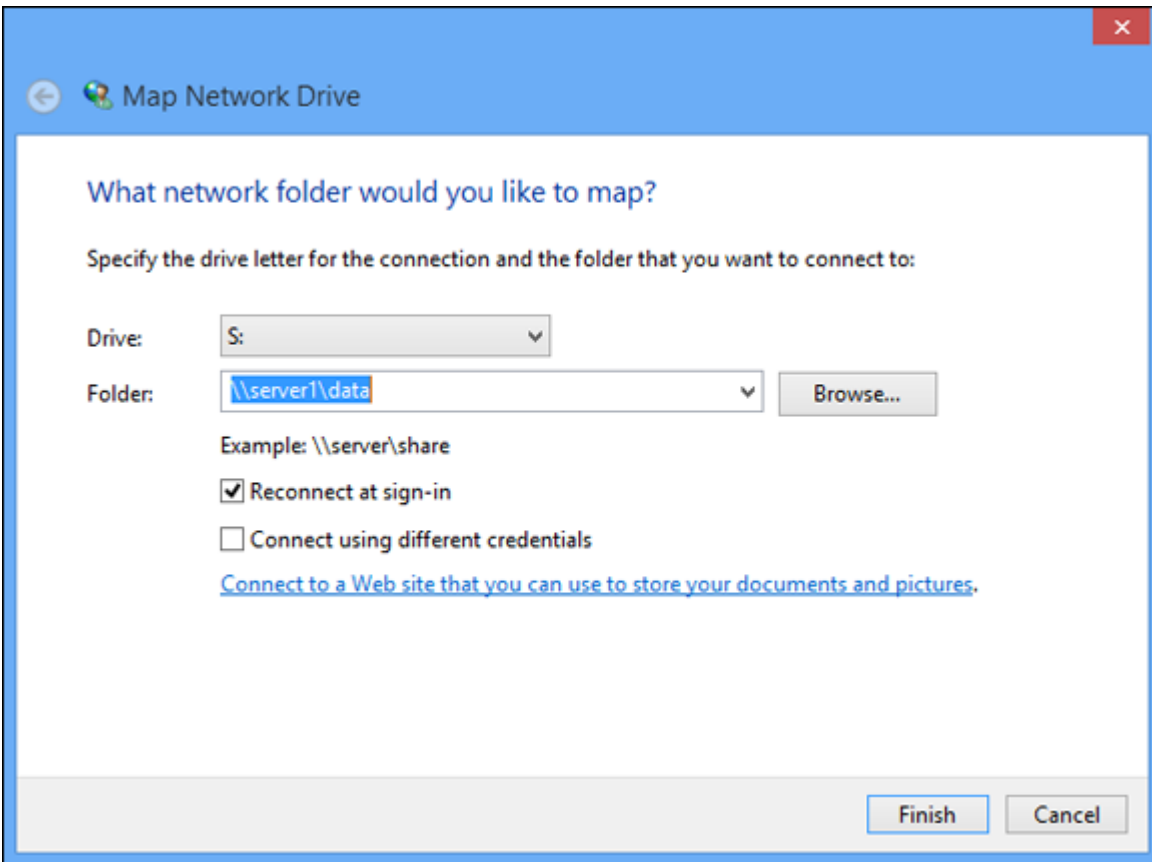
**TIP**

Using UNC paths means that you have to be aware of the exact names used for resources on the network, including hidden shares. When you get used to the computer names and share names on the network, you'll find that the `Run` command is quicker than waiting to see the list of computers in Network Neighborhood or My Network Places.

### *Mapping a network drive*

You may also connect to shares by mapping drives. If you find that you are constantly connecting to the same resource, you may want to map a drive for the sake of simplicity. The idea of mapping a drive is that, in the end, you have a new drive letter in your “This PC” folder that points to the UNC path of the resource. After the drive is mapped, anytime you want to access the folder on the network, go to “This PC” and double-click the mapped drive.

To map a drive, right-click This PC and then choose Map Network Drive. In the Map Network Drive dialog box, select the letter for the drive you want to create and then type the UNC path to the shared resource into the Path text box. You may also choose the option to re-create this drive mapping the next time you log on so that you do not have to do this again. [Figure 3-16](#) shows the Map Network Drive dialog box.



**FIGURE 3-16:** Mapping a network drive in Windows.



**ON THE  
WEB**

Lab 3-4 allows you to practice sharing resources and connecting to resources. Lab 3-4 can be found on the companion website at [www.dummies.com/go/aplusaio](http://www.dummies.com/go/aplusaio).

## *Administrative shares*

An *administrative share* in Windows is a default share that exists hidden on the network, and only administrators have permission to connect to them. These administrative shares are used by administrators, but also by Windows to copy files between systems that are needed in the background in some cases. For example, if you connect to a shared printer on the network, the printer driver may be copied between the two systems if it is needed.

Here is a summary of some of the administrative shares that exists in Windows:

- » **C\$:** The root of drive C is shared as `c$`. Actually, the root of any drive on the system has an administrative share. For example, `c$`, `d$`, and `e$` (if you had a C, D, and E drive).
- » **admin\$:** The directory you installed Windows into (typically `c:\windows`) is shared as `admin$`.
- » **ipc\$:** A communication channel for systems to communicate with one another.

## *Sharing Printer Resources*

You share printers in much the same way that you share folders on your system. After you install the printer and configure the settings so that the printer functions properly, it is time to share it.

### *Sharing a printer in Windows*

To share a printer in Windows 7 or Windows 8.1, follow these steps:

1. **Navigate to the Control Panel:**
  - *Windows 10:* Click the Start button, then type **control**. Choose Control Panel from under the Best Match section.
  - *Windows 8.1:* Right-click the Start icon and choose Control Panel.
  - *Windows 7/Vista:* Click Start ⇒ Control Panel.
2. **In the Control Panel, select Hardware and Sound ⇒ Devices and Printers.**
3. **Right-click the printer you want to share and choose Printer Properties.**
4. **Click the Sharing tab.**
5. **Enable the share by selecting Share This Printer and then give a share name, such as “Canon” or “HP.”**

## 6. Click OK.

When sharing printers, all the same rules for sharing folders apply as far as the share name goes and how to create hidden shares.

## *Installing a network printer in Windows*

To print, or connect, to a shared printer out on the network, you have to install a network printer on your Windows client that points to the UNC path of the shared printer. A *network printer* in Windows is a printer installed that refers to a shared printer on the network. When you print to a network printer, the print job is sent to the computer that has the printer installed and prints from the print device connected to that system.

You can install a network printer in a number of ways. The two most popular methods are through the Add a Printer Wizard and through the `Run` command, depending on the network setup. To install a network printer using the wizard, run the wizard from the Printers folder. The wizard starts up and walks you through connecting to a shared printer. The following section shows you how to install a printer that points to a network location.

In Windows 7, Vista, and Windows 8.1, you install a network printer through the Control Panel by following these steps:

### 1. Navigate to the Control Panel:

- *Windows 10*: Click the Start button, then type **control**. Choose Control Panel from under the Best Match section.
- *Windows 8.1*: Right-click the Start icon and choose Control Panel.
- *Windows 7/Vista*: Click Start ⇒ Control Panel.

### 2. In the Control Panel, select Hardware and Sound ⇒ Devices and Printers.

### 3. Click the Add a Printer button on the toolbar.

### 4. Select the Add a Network, Wireless, or Bluetooth Printer option.

5. If the printer appears in the list, choose it. If it does not appear in the list, choose the **The Printer That I Want Isn't Listed** option.
6. Type the UNC path to the printer and click **Next**.
7. Click **Finish**.

## *Installing a network printer by using Point and Print*

One of my favorite ways to install a network printer on a client is by taking advantage of Point and Print within Windows. Point and Print is a feature that copies the printer driver from one system to another as soon as you connect to the printer — no matter how you connect to the printer! What method is quickest to connect to the printer? Using the UNC path in the `Run` command!

After you type the UNC path of the shared printer you want to connect to, Windows asks whether you want to install the printer on your system. When you choose **Yes**, a new printer is created in the **Printers** folder without you having to run through the wizard. The printer driver is automatically copied from the system sharing the printer to your local system.

To install a printer by using Point and Print, follow these steps:

1. Place your cursor in the **Search** box in **Windows 7**, or in **Windows 8.1** simply go to the **Start** screen.
2. Type `\\computername\PrinterShareName`, where *computername* is the name of the system that is sharing the printer, and *PrinterShareName* is the name of the shared printer.
3. When asked if you want to install the printer, click **Yes**.

The printer is now installed and ready to print to.

## *Networking with Windows*

Now it is time to look at some common tasks performed in Windows as it relates to network settings. This section covers topics such as changing your computer name or workgroup, joining a domain, home groups, and network profiles.

## *Computer name and workgroup*

The first thing you should know is how to change your computer name and workgroup in Windows 7 and Windows 8.1. To change your computer name and workgroup, follow these steps:

### **1. Navigate to the Control Panel:**

- *Windows 10:* Click the Start button, then type **control**. Choose Control Panel from under the Best Match section.
- *Windows 8.1:* Right-click the Start icon and choose Control Panel.
- *Windows 7/Vista:* Choose Start ⇒ Control Panel.

### **2. In the Control Panel, choose System and Security and then choose System.**

You can see the computer name toward the bottom of the screen.

### **3. To change the computer name, click the Change Settings link that appears on the right, next to the computer name.**

### **4. Click the Change button.**

The Computer Name Changes dialog box appears, allowing you to type a new computer name.

## *Joining a domain*

A *domain* in Windows is a security boundary that allows an administrator of the network to administer any system within that domain. In order for your computer to fall into this administrative boundary, you must join your Windows computer to the domain.

To join a domain on a Windows system:

### **1. Navigate to the Control Panel:**

- *Windows 10*: Click the Start button, then type **control**. Choose Control Panel from under the Best Match section.
  - *Windows 8.1*: Right-click the Start icon and choose Control Panel.
  - *Windows 7/Vista*: Click Start ⇒ Control Panel.
2. **In the Control Panel, choose System and Security and then choose System.**

In the computer name, workgroup, and domain section you will Choose the domain you are a part of. If it shows a workgroup, then you are not part of a domain.
  3. **To join a domain, click the Change Settings link that appears on the right, next to the computer name.**
  4. **Click the Change button.**

The Computer Name Changes dialog box appears, allowing you to specify the domain you want to join.

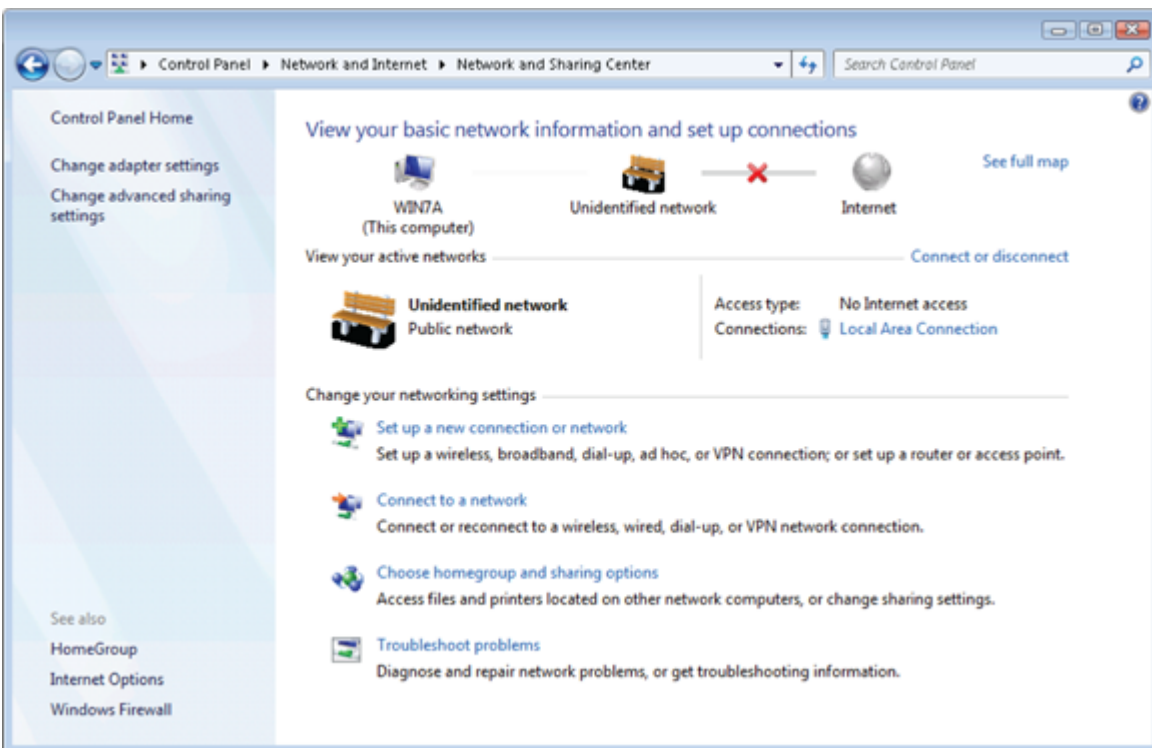
## ***Changing IP settings***

To change your TCP/IP settings in Windows 7 and Windows 8.1, follow these steps:

1. **Locate the network connections:**
  - *Windows 10*: Click the Start button, then type **control**. Choose Control Panel from under the Best Match section. Choose Network and Internet ⇒ Network and Sharing Center ⇒ Change Adapter Settings.
  - *Windows 8.1*: Right-click the Start icon and then choose Control Panel ⇒ Network and Internet ⇒ Network and Sharing Center ⇒ Change Adapter Settings.
  - *Windows 7/Vista*: Click Start ⇒ Control Panel ⇒ Network and Internet ⇒ Network and Sharing Center (see [Figure 3-17](#)) and then click the Change Adapter Settings link on the left.

2. **Right-click your network connection, which appears as local area connection (Windows 7) or Ethernet (Windows 8.1/Windows 10), and then choose Properties.**
3. **Click the Properties button to view the network components associated with your local area connection.**
4. **Select Internet Protocol Version 4 (TCP/IPv4), and then choose Properties.**

Here you can set your IP address, subnet mask, default gateway, and primary DNS server setting. After you set the values, click OK to exit your way back to Windows.



**FIGURE 3-17:** Network and Sharing Center window in Windows.

## *Homegroup*

A new networking feature that started with Windows 7 and continued with Windows 8.1 is the Homegroup feature. A homegroup in Windows makes it easy to share network resources, such as folders and printers, to other Windows systems in your homegroup. For example, when you share a printer on a system in a homegroup, that printer is automatically installed



on any system that joins the homegroup! To create a homegroup in Windows, follow these steps:

**1. Locate Network and Internet:**

- *Windows 10:* Click the Start button, then type **control**. Choose Control Panel from under the Best Match section. Choose Network and Internet.
- *Windows 8.1:* Right-click the Start icon and then choose Control Panel ⇒ Network and Internet.
- *Windows 7/Vista:* Click Start ⇒ Control Panel ⇒ Network and Internet.

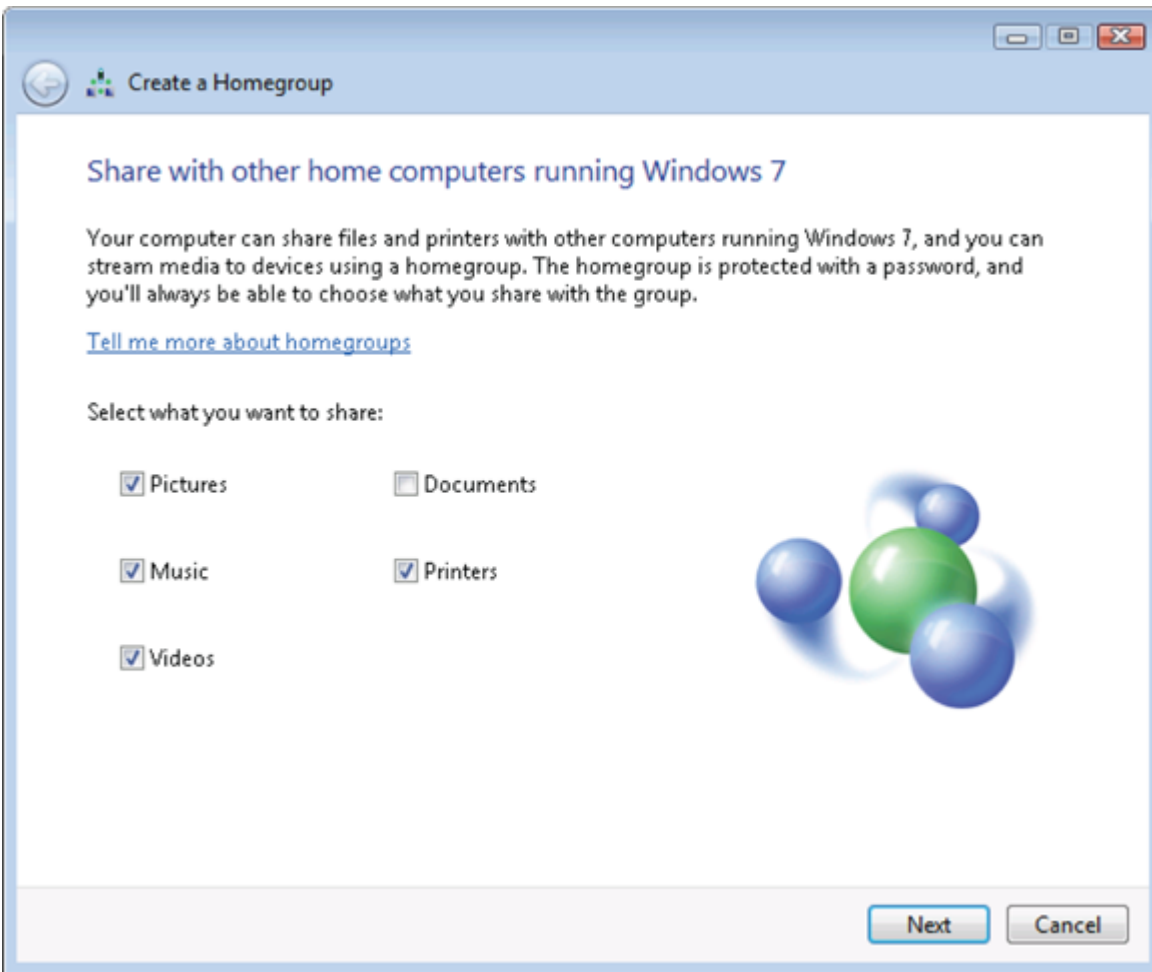
**2. Click the Homegroup link.**

If you are unable to create a homegroup with the Create a Homegroup button, you most likely must change your network location to Home by clicking the What Is a Network Location link. Click the link and set the location to Home; then the Create a Homegroup Wizard is automatically run.

**3. In the Create a Homegroup Wizard, you are asked what resources should be shared to members of the homegroup (see [Figure 3-18](#)). Click Next.**

You are presented with a password that you must write down. This password is needed by anyone who wants to join his or her computer to the homegroup at a later time.

**4. Click Finish.**



**FIGURE 3-18:** Configuring a homegroup.

After you have created the homegroup, anyone can join their Windows system to the homegroup by following similar steps. You can also share folders to the Homegroup by right-clicking the folder and choosing Share With  $\Rightarrow$  Homegroup (Read). Or, you could choose Share With  $\Rightarrow$  Homegroup (Read/Write).

If you need to view the homegroup password or leave the homegroup, navigate to the Control Panel, click the Network and Internet link, and then click the Homegroup link. Within the Homegroup Settings window, you can view or print your password, change the homegroup password, leave the homegroup, or modify the sharing settings with the homegroup.

## *Network profiles*

One of the great features of Windows is the network profiles feature. When a user connects to a network such as a wireless network, he or she is prompted as to what type of network it is — a **home, work, or public network**. The location the users set determines the networking features that are configured. For example, if the user sets the location to work, the firewall on his system could be automatically disabled. Yet if he connects to a wireless network at a hotel and chooses public as the location, you as an administrator can set the public network profile to have a firewall enabled. The benefit of these profiles is that you can configure a system in different ways, depending on what profile is selected.

As an example of a network setting that can be set, you can set whether your system will share files with a particular profile. You can also set whether other systems on the network can see your system (known as *network discovery*) and access your shared folders.

To configure these settings on a per-profile basis, follow these steps:

**1. Locate the Control Panel:**

- *Windows 10*: Click the Start button, then type **control**. Choose Control Panel from under the Best Match section.
- *Windows 8.1*: Right-click the Start icon and then choose Control Panel.
- *Windows 7/Vista*: Click Start ⇒ Control Panel.

**2. Click the Network and Internet link.**

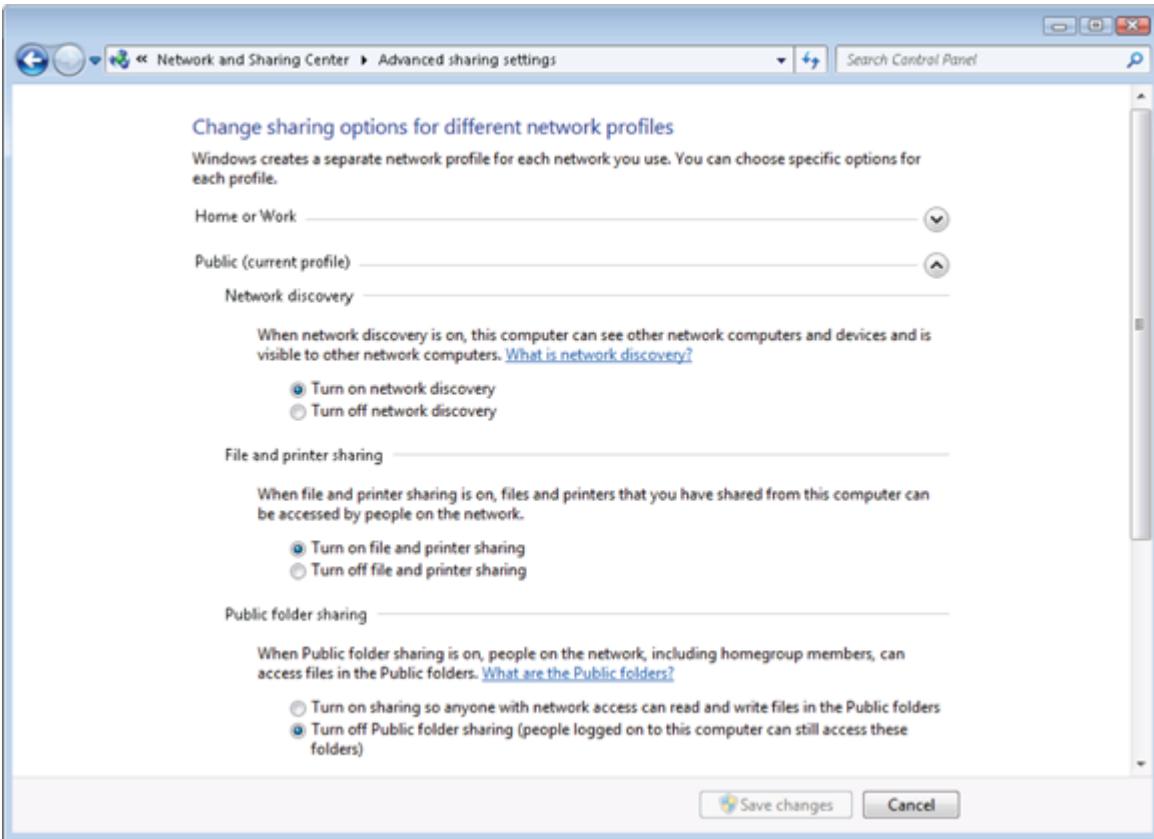
**3. Click the Network and Sharing Center link.**

**4. In the Network and Sharing Center window, click the Change Advanced Sharing Settings link on the left side.**

The Advanced Sharing Settings appear (see [Figure 3-19](#)).

**5. Choose to turn off Network Discovery and File and Printer Sharing for the public profile, but turn them on for the home and work profiles.**

**6. Close all windows.**



**FIGURE 3-19:** Advanced sharing settings.

## *Firewall settings*

Another common network setting you will need to configure is the firewall feature. The Windows firewall is designed to limit what traffic can reach your system.

### *Basic configuration*

To configure the Windows firewall, follow these steps:

#### **1. Locate the Control Panel:**

- *Windows 10:* Click the Start button, then type **control**. Choose Control Panel from under the Best Match section.
- *Windows 8.1:* Right-click the Start icon and then choose Control Panel.
- *Windows 7/Vista:* Click Start ⇒ Control Panel.

#### **2. Click the Network and Internet link.**

**3. Click the Network and Sharing Center link.**

**4. Choose Windows Firewall at the lower left of the dialog box.**

The firewall can be enabled or disabled for different network profiles by clicking the Turn Windows Firewall On (or Off) link.

**5. Choose whether you want the firewall to be on or off for each of the network profiles.**

You can also specify whether you want to be notified if a program is blocked by the firewall.

### ***Firewall exceptions***

From time to time, you may need to add exceptions to the firewall; exceptions are selected traffic that you decide to let through the firewall. For example, my son wanted to host his own Minecraft server, so I had to allow the Minecraft traffic to pass through the firewall on his system. To add exceptions to the firewall, click the Allow a Program or Feature through the Firewall link, which is found in the Windows firewall dialog box. From there you can choose to create an exception by port number and specify the port value for the type of traffic you want to allow through the firewall. For example, if you want to remotely administer the system with the remote desktop feature, you will need add the exception for TCP port 3389.

### ***Network card properties***

You can configure a number of settings on your network cards. These settings are typically found in the properties of the network card in Device Manager. The following are some common network card settings, also known as properties:

- » **Duplex setting:** Within the properties of your network card, you can set whether you want the card to run in full-duplex mode, half-duplex, or autodetect. With full-duplex, the card can send and receive at the same time; with half-duplex, it can only send or receive at one time. If you set the card to autodetect, it will determine the best setting based on the network you connect it to.

- » **Speed:** Most cards are multispeed cards and support either 10-Mbps, 100-Mbps, or 1000-Mbps speeds. You can set the speed or again leave it at autodetect.
- » **Wake on LAN:** A network card that supports wake on LAN functionality can wake the system out of Sleep mode when it receives a special network message.
- » **PoE:** Power over Ethernet (PoE) allows the system to receive power through the Ethernet cable connected to the system.
- » **QoS:** Quality of service (QoS) settings allow the traffic to be optimized by limiting bandwidth usage for different types of traffic.
- » **BIOS (on-board NIC):** In the BIOS settings for the computer you can enable or disable the on-board network card. You may want to do this if you purchased a newer card and want to disable the old card to ensure it is not being used for network communication.

## *Wireless locator*

You can use the Wireless Locator icon found on the right side of the Taskbar. The wireless locator allows you to click the icon on the Taskbar to view a list of wireless networks. To connect to a wireless network, you click the name of the wireless network and you are then prompted for the password for that wireless network. If you type the correct password, you are then granted access.

If a wireless network is present that has the SSID broadcasting disabled, in Windows, you will see an entry for the network in the wireless locator that says `Other Network`. When you choose `Other Network`, you must type the name of the SSID. If that is supplied correctly, you are then prompted for the password.

## *Establishing a connection*

Windows allows you to connect to a wealth of other network environments, with the most popular being establishing a secure VPN connection to encrypt data across an untrusted network, or a simple dial-up connection.

You can create a dial-up or VPN connection by clicking the Set Up a New Connection or Network link found in the Network and Sharing Center. The following lists some common types of connections and defines their purpose:

- » **VPN:** A virtual private network (VPN) connection is used to connect the IP address of a secure server across the Internet that can encrypt data sent between your system and that server.
- » **Dial-up:** A dial-up connection is used to connect to the phone number of a server that can then grant you access to a network over the phone lines. You need to have a modem installed on your system to dial-up to this server.
- » **Wireless:** A wireless connection is established by adding a wireless network card to the system.
- » **Wired:** A wired connection is created when you add a wired network card to the system.
- » **WWAN:** A wireless wide-area network (WWAN) allows access to the Internet through cellphone towers and cellular phones.

## *Remote access technologies*

Remote access is a common topic and feature desired by IT professionals today. Remote access is the idea that you want to access a system from across the Internet. There are a number of remote access protocols that can be used for remote access:

- » **Remote desktop connection:** Although not a physical type of connection, but more of a remote access technology that allows you to connect to your computer from across the network or Internet and use your computer when you are physically away from it. Keep in mind that someone connecting must have a username and password and be given permission to remote into a system.
- » **Remote assistance:** Remote assistance is a remote access feature that allows someone to invite you to connect to her computer and help her fix a problem. The person can disconnect you at any time if she so

chooses. The person you invite to help can view what you are doing and chat with you, or can take control (if you allow) and show you how to perform at task.

- » **Telnet:** Telnet is a common remote access protocol used by network administrators to remotely connect to a router and switch and perform administrative duties. Telnet is an older protocol and not recommended as the communication, including logon traffic, is unencrypted.
- » **SSH:** Secure shell (SSH) is the secure replacement protocol to Telnet that allows an administrator to remotely connect to a router or switch while the traffic is encrypted (including authentication traffic).
- » **Third-party tools:** There are a number of third-party tools that give you remote access to a system, such as WinVNC. The key point is to verify that traffic is encrypted so that someone cannot monitor the traffic and see your username and password as you log on with the third-party software.

## *Public/shared devices*

Another common practice today is to share devices on the network so that other users can access those devices. An example would be to use AirPrint, a protocol that allows you to print to printers from your mobile device. The following is a summary of features that allow working with shared devices:

- » **TCP:** You can connect to printers on the network or across the Internet with the Internet Printing Protocol (IPP) over TCP port 631.
- » **Bonjour:** Bonjour is a communication protocol that allows devices on a network to communicate with one another. It is a common method on home networks to allow Apple devices to connect to printers on the network.
- » **AirPrint:** An Apple protocol used to access a printer on the network from an iOS device or MacOS device.



When working with shared devices, you want to consider user authentication on the device and how the authentication works on the device. Is the authentication information being stored? If so, is it encrypted? Also be aware if any information is being cached on the hard drive. Technologies that use hard-drive caching can potentially store sensitive information that is retrieved at a later time.

## *Understanding Windows Services*

In this section, I introduce you to the concept of a service within the OS and then give an overview of some of the most popular services found in Windows.

A *service* is a software component within the OS that provides a specific feature. For example, the spooler service provides printing functionality. For you to print, you must have the spooler service running.

There are a number of settings you can configure with services, such as set the service to start automatically when Windows starts, or have it set to manually start, which means that as an administrator you need to start the service. You can also start and stop services in order to troubleshoot that aspect of the operating system — it is like rebooting that part of the operating system!

### *Restarting a Windows service*

To stop, start, or restart a service in Windows, follow these steps:

#### **1. Locate the Control Panel:**

- *Windows 10:* Click the Start button, then type **control**. Choose Control Panel from under the Best Match section.
- *Windows 8.1:* Right-click the Start icon and then choose Control Panel.
- *Windows 7/Vista:* Click Start ⇒ Control Panel.

#### **2. Click the System and Security link.**

3. Click the **Administrative Tools** link to open the **Administrative Tools** window.
4. Double-click the **Services** icon to launch the **Services** console.
5. From the **Services** console, stop, start, or restart a service by right-clicking the service and then choosing the appropriate command from the contextual menu.

After you know how to stop and start a service, the next step is to understand some of the key services that exist within the Windows OS and what the service offers to the system.

### *Server service*

One of the critical services responsible for the networking of the Windows OS is the Server service, which provides File and Printer Sharing capabilities. So, if you want to print to a printer that is shared on computer A from your system, computer A needs to have the Server service running to allow your system to connect to it.

### *Workstation service*

The Workstation service — the exact opposite of the Server service — is responsible for making the connection to the system running the Server service. Compare this with the example in the preceding section: If you want to print to a printer on computer A, the Workstation service on your computer sends the request to the Server service on computer A.

### *DHCP Server service*

The *DHCP Server service* handles DHCP server functionality: that is, a server that hands out IP addresses to clients on the network. This service must be running if you want the DHCP server to hand out the IP addresses to network clients. **Note:** This service exists only on Windows Servers and not on Windows client OSes.

### *Print Spooler service*

As I mention earlier, the *Print Spooler* service is responsible for the printing environment in Windows. If this service is not running, you

cannot print.

## *Messenger service*

The *Messenger service* is an older service found on older versions of Windows that is responsible for sending and receiving messages within the OS. For example, some features of the OS allow an alert to be sent to the network administrator — and the Messenger service is responsible for the message (alert) being sent. You can send a message to another user on the network at any time via the following command at a command prompt:

```
Net send BOB "Hi there"
```

The above command sends a message to a user or computer called BOB, and the message that appears on Bob's screen reads Hi there. For Bob to receive the message, your computer and Bob's computer need to have the Messenger service running.

## *Getting an A+*

This chapter discusses the different networking components that allow a Windows OS to function in a networking environment.

- » Four major networking components are required in Windows networks:
  - A network client
  - A network adapter
  - A common protocol
  - A service
- » TCP/IP is the most popular networking protocol used today. When installing TCP/IP, you need to configure the following:
  - An IP address
  - A subnet mask
  - A default gateway

- » The NetBEUI protocol is a nonroutable protocol used on small networks.
- » In Microsoft networking environments, to allow users to connect to your hard drive or printer, you must install the File and Printer Sharing service.
- » You may use the `ipconfig` command in Windows to view your TCP/IP configuration.
- » The `ping` command is used to send test messages to a remote system to verify that communication can take place on that system.

## *Prep Test*

**1. What networking component allows you to connect to a Windows Server?**

- (A) File and Printer Sharing service
- (B) Client Service for Netware
- (C) TCP/IP
- (D) Client for Microsoft Networks

**2. There is a shared folder named `public` on a computer named `Server1`. What is the syntax to connect to the shared resource via the UNC path?**

- (A) `\\server1\public`
- (B) `\\server1\data`
- (C) `\\data\server1`
- (D) `\server1\data`

**3. Which of the following IP addresses has a default subnet mask of `255.255.255.0`?**

- (A) `10.45.65.78`
- (B) `132.107.2.34`
- (C) `48.123.45.67`

(D) 216.83.24.56

**4. You would like other people in the office to be able to access the printer that is attached to your Windows 8.1 computer on your small network. Which networking component must you install?**

- (A) Client for Microsoft Networks
- (B) Client Service for Netware
- (C) File and Printer Sharing for Microsoft Networks
- (D) NetBEUI

**5. Which of the following is an example of a Class B IP address?**

- (A) 164.34.56.8
- (B) 12.45.76.2
- (C) 202.34.65.32
- (D) 125.67.6.7

**6. What two properties of TCP/IP must be configured to communicate with other hosts on a small, local network?**

- (A) IP address
- (B) DNS server
- (C) Default gateway
- (D) Subnet mask

**7. A user tries to connect to a shared resource called `data` on `server1` by using the UNC path `\\server1\data` but is unsuccessful. The user knows the IP address of `server1` and can successfully ping it. What is the problem?**

- (A) The user should use `\\data\server1`.
- (B) The client computer is not configured to query the WINS server.
- (C) The client computer is not configured to query the DNS server.
- (D) The user needs to install TCP/IP.

**8. Which utility allows you to see the path that information may take when communicating with a remote system?**

- (A) `ipconfig.exe`
- (B) `tracert.exe`
- (C) `winipcfg.exe`
- (D) `arp.exe`

**9. Which of the following TCP/IP settings are required to connect to the Internet? (Choose all that apply.)**

- (A) IP address
- (B) WINS
- (C) Subnet mask
- (D) Default gateway

**10. Which resolution technique is used to resolve the IP address to a MAC address?**

- (A) DNS
- (B) WINS
- (C) ARP
- (D) `ipconfig.exe`

**11. Which utility allows you to see the IP address information on a Windows 7 computer?**

- (A) `netstat.exe`
- (B) `ipconfig.exe`
- (C) `tracert.exe`
- (D) `arp.exe`

**12. Which service is responsible for automatically assigning IP address information to each computer on the network?**

- (A) DNS

- (B) WINS
- (C) `netstat.exe`
- (D) DHCP

**13. You verified that you have a network adapter installed and an appropriate client, but you cannot connect to computer B across NetBEUI. What could be the problem?**

- (A) You have the wrong IP address assigned to the computer.
- (B) Computer B is not running NetBEUI.
- (C) You should check the frame type on your computer.
- (D) You need to install File and Printer Sharing to connect to another computer.

**14. When you use `ipconfig.exe`, you do not see the IP address of the DHCP server that has given you the IP address. What should you do?**

- (A) Use `ipconfig /renew` at the command prompt.
- (B) Use `ipconfig /all` at the command prompt.
- (C) Ping the IP address of the DHCP server.
- (D) Use `ipconfig /release` at the command prompt.

**15. You installed a printer and want to share it out to the network. How can you do this?**

- (A) Use `net print` at the command prompt.
- (B) Install the Client for Microsoft Networks.
- (C) Configure the DHCP server on the network.
- (D) Right-click the printer in the Printers folder and choose the Sharing command.

**16. Which service is responsible for converting [www.wiley.com](http://www.wiley.com) to an IP address?**

- (A) DHCP

- (B) DNS
- (C) WINS
- (D) ARP

**17. You want to share the data folder as a resource to be used only by network administrators. How should you do this?**

- (A) Hide the share by naming it `data$` and then set up the permissions so that only administrators have access. Tell the administrators the UNC path.
- (B) Don't share the folder; tell the administrators to go to the local computer to access the resource.
- (C) Set up the share permissions so that only administrators have access to the share.
- (D) Share the resource and don't set any permissions.

**18. You are installing a small network with six Windows 8.1 computers that will share resources between one another. You want to use a Class B address when configuring the IP address on the first system; which address would you use?**

- (A) 129.14.54.10
- (B) 127.0.0.1
- (C) 192.168.1.43
- (D) 24.54.84.57

**19. You are troubleshooting why Bob's computer does not have Internet access so you use the `ipconfig` utility to view his TCP/IP settings. You notice his IP address is 169.254.34.56. Why can't Bob access the Internet?**

- (A) There is a problem with the DNS server.
- (B) There is a problem with the router.
- (C) There is a problem with the DHCP server.
- (D) There is a problem with the firewall.



# Answers

1. **D.** To connect to a resource, you must have the appropriate client running. In this example, you are logging into a Windows server, so you must load the Client for Microsoft Networks. See “[Network client](#).”
2. **A.** To connect to a shared resource on the network use the UNC path. The proper syntax for a UNC path is `\\servername\sharename`. Review “[Using a UNC path](#).”
3. **D.** 216.83.24.56 is an example of a Class C address, whose default subnet mask is 255.255.255.0. The other addresses are Class A and Class B, which have different default subnet masks. Check out “[Subnet mask versus CIDR](#).”
4. **C.** File and Printer Sharing must be installed to allow someone to connect to your resources. Take a look at “[Enabling File and Printer Sharing in Windows](#).”
5. **A.** The number in Class B addresses' first octet ranges from 128 to 191. The number in Class A addresses' first octet ranges from 1 to 126, and the number in Class C IP addresses' first octet ranges from 192 to 223. Peek at “[IP address](#).”
6. **A, D.** Because the computer is functioning on a small LAN with no router, all you need to configure the functionality of TCP/IP is the IP address and subnet mask. Because no information leaves the network, you do not have to configure a default gateway. Look over “[The TCP/IP Protocol](#).”
7. **B.** The computer name, `server1`, must be converted to an IP address. WINS is the service that maintains a database that holds computer names and matching IP addresses. Study “[WINS](#).”
8. **B.** `tracert.exe` is the utility used to see the number of networks between you and the remote host. `ipconfig.exe` and `winipcfg.exe` display the TCP/IP configuration. Refer to “[TRACERT/traceroute](#).”

9. **A, C, D.** To participate on the Internet, you need an IP address, a subnet mask, and a default gateway. The default gateway is the IP address of the router that sends information off the network. *Examine “[Configuring TCP/IP in Windows](#).”*
10. **C.** Address Resolution Protocol (ARP) converts the IP address to the network card address (MAC address). DNS and WINS convert different types of names to an IP address. *See “[ARP](#).”*
11. **B.** `ipconfig.exe` is the utility run on Windows products to view TCP/IP configuration. `winipcfg.exe` is the utility on Windows 95 and Windows 98. *Review “[IPCONFIG/ifconfig](#).”*
12. **D.** Dynamic Host Configuration Protocol (DHCP) is a service on a server that automatically assigns IP address information to each computer on the network, saving the network administrator from having to manually configure each computer. *Check out “[DHCP Server service](#).”*
13. **B.** If you have a client and a network adapter installed, and they are working correctly, the reason why you cannot connect across NetBEUI is because the person on the other end is using a different protocol. *Peruse “[NetBEUI](#).”*
14. **B.** Without switches, `ipconfig.exe` displays only the IP address, subnet mask, and default gateway. Use the `ipconfig /all` switch to view all TCP/IP configurations, including the DHCP server that assigned your computer an IP address. *Take a look at “[IPCONFIG/ifconfig](#).”*
15. **D.** After you install File and Printer Sharing, you need to right-click the printer and choose the Sharing command. *Peek at “[Sharing Printer Resources](#).”*
16. **B.** DNS is responsible for converting fully qualified domain names to IP addresses. WINS converts the computer name to an IP address, DHCP is responsible for automatic configuration of TCP/IP, and ARP is responsible for converting IP addresses to MAC addresses. *Look over “[DNS](#).”*

17. **A.** The best way to be sure that no one except network administrators can access a shared resource is to share the resource and set the proper permissions. When you share the resource, though, it may be best to hide it from the network by making it a hidden share so that no one tries to sneak into it. *Study “[Sharing File System Resources](#). ”*
18. **A.** Answer is A because Class B addresses have a first octet that ranges between 128 and 191. Class A addresses have a first octet that ranges between 1 and 127, and Class C addresses have a first octet that ranges between 192 and 223. *Refer to “[IP address](#). ”*
19. **C.** Bob’s computer is using an APIPA address which is automatically assigned to the system when there is a problem contacting a DHCP server on the network. *Examine “[Special addresses](#). ”*

# Chapter 4

## Configuring Internet Access and SOHO Networks

---

### IN THIS CHAPTER

- » Getting connected to the Internet
  - » Working with TCP/IP technologies on the Internet
  - » Configuring Internet settings with Internet Explorer
  - » Installing a Small Office/Home Office (SOHO) Network
  - » Working with firewall devices to protect your computer
- 

In this chapter, you examine how to connect to the Internet and discover some of the basics of how it works. This chapter is chock-full of terminology that you need to be familiar with as well as different methods available to access the Internet. Because the Internet now plays such an integral part in many people's lives, as a CompTIA A+ Certified Professional, you should be familiar with where it came from — and how to connect to it.

## *Understanding the Internet*

The Internet was originally created and implemented by DARPA (Defense Advanced Research Projects Agency; often referred to as just *ARPA*) in response to a U.S. Department of Defense (DoD) request. At the time, the DoD was concerned about its centralized communications network. Most communications were relayed through a central computing system or hub, and damage to that system could stop computer communication. To avoid this problem, the DoD gave ARPA the responsibility of devising a new system.

The first thing that ARPA had to do was to create communication protocols that would allow computers to talk to each other in a new and nonstandard, decentralized manner, and ARPA needed a small network on which it could test and develop the new protocols. It eventually interconnected four hosts, which formed the start of the ARPANET.

ARPANET (and now the Internet) was defined by a series of standards that are currently being put forth by the Internet Architecture Board (IAB), which represents the governing body of the Internet. These Internet standards are defined by IAB but are discussed in RFC (Request for Comments) documents. The first RFC defined how the initial hosts on the ARPANET would send to and receive data from each other.



**TIP**

All RFCs — currently, more than 5,500 — are available from [www.ietf.org](http://www.ietf.org). Technologies in RFCs sometimes make it into STD (Standards) documents, of which there are currently fewer than 70. An index of the standards can be found at

[www.rfc-editor.org/std-index.html](http://www.rfc-editor.org/std-index.html)

During the 1970s, protocols were created and evolved, allowing for support of more and more services over ARPANET, and the number of members continued to increase. Most ARPANET members were locations that did research for ARPA — mainly universities and research centers. Terminal connections via Telnet were created, as was the fashion of using the @ character (meaning *at*) as a separator between username and mail server for email addresses. Emoticons were soon to follow, starting with joke markers, such as -) (tongue in cheek) in the late 1970s, and the first smileys :-) in the early 1980s. Now we have emoji icons that are little yellow icons showing different emotions and expressions and sometimes hand signals like a thumbs-up.

During the 1980s, several major events occurred:

» TCP/IP became the standard communication protocol.

- » The term *Internetwork*, truncated to just *Internet*, became the name of the network.
- » Many operating systems were standardized on TCP/IP.
- » The National Science Foundation took over management of the Internet.
- » The IAB was established to manage accepted standards on the Internet.

Also during 1980s, other countries started to join their national networks to the U.S. Internet, making it a true world-wide network. Several new application protocols were created to allow communication, such as NNTP (Network News Transfer Protocol) and IRC (Internet Relay Chat). This was also the decade that saw the first Internet worm released — namely, the Morris Worm, which was named for its creator.

*TCP/IP* — Transmission Control Protocol/Internet Protocol — is the protocol suite that is used by the Internet, but it comprises many different protocols that function at different levels of the network model. There are network protocols, transport protocols, and application protocols. In fact, the number of protocols is limitless. Many key protocols are discussed in earlier chapters (see Book 7, [Chapter 3](#), and Book 8, [Chapter 1](#)), but this chapter covers some of the others, such as

- » **SMTP:** Simple Mail Transport Protocol
- » **POP3:** Post Office Protocol version 3
- » **HTTP:** Hypertext Transfer Protocol
- » **FTP:** File Transfer Protocol
- » **IMAP:** Internet Message Access Protocol



FOR THE  
EXAM

TCP/IP — the communication protocol used on the Internet — is actually a suite of protocols that covers all aspects of the communication process.

In the 1990s, the biggest single change to the Internet was caused by CERN (Conseil Européen pour la Recherche Nucléaire, or the European Council for Nuclear Research) developing a new method of linking documents stored on different servers. CERN modified SGML (Standard Generalized Markup Language), created a new language called HTML (Hypertext Markup Language), and named the technology the World Wide Web. This single technology changed the face of the Internet, which went from a method of linking documents for information to a conduit for shopping, personal expression, media production and delivery, and untold other things.

Since 2000, technologies created for and used over the Internet have steadily risen to allow for remote access, collaboration, file sharing, streaming media, and VoIP (Voice over Internet Protocol). Government services and major corporations have all embraced the Internet as a major method of communicating with clients, and people in general have changed how they communicate, using instant messaging and social networking sites. Internet gaming has become popular, with software companies generating steady revenue streams from monthly gaming fees. Today, if the Internet disappeared, many people would be at a loss to figure out how to communicate with one another.

Many countries now offer public access terminals for the Internet in convenient locations, such as libraries. Users can connect to the Internet through these public access terminals, WiFi hotspots, and any number of other methods. Some cities have gone so far as to set up city-wide public wireless access.

The Internet has evolved from something small to become what we now know as the Internet. Even today, the Internet is constantly evolving, with new protocols created daily and new uses for the technology limited only

by imagination. I wonder what the Internet will look like by the end of the next decade.

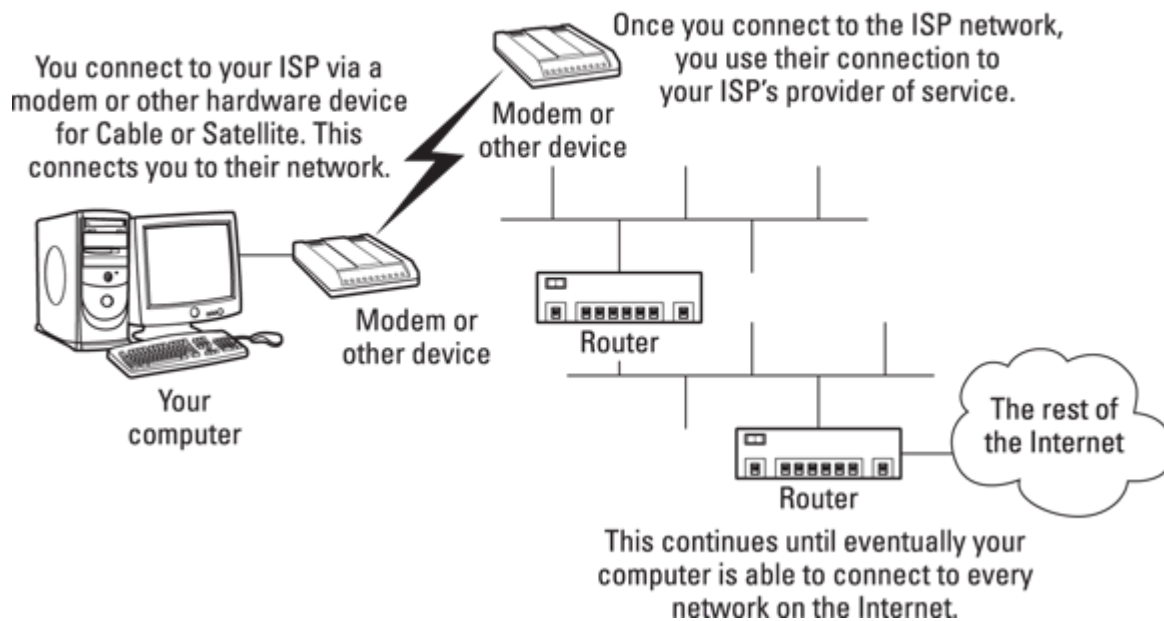
## *Using an ISP*

Essentially, the Internet is a large, routed network, with technology similar to the networks found in a large corporation. The main difference between the Internet and a corporate network, though, is that all the small networks that make up the Internet are conjoined, but corporate networks are kept private. To access the Internet, you must access one of the networks that are connected to the Internet. These networks are run by Internet service providers (ISPs), which are in place simply to allow you to access the Internet. [Figure 4-1](#) illustrates how a connection to the Internet works. In order to get connected to the Internet, the following would occur:

1. Connect your computer to your ISP's network by using a communication device, such as a modem or router.
2. The ISP connects its network to its provider's network by using a router and a communication link, such as a leased Telco line.
3. Eventually, a connection is made to part of the Internet backbone, which allows connections to every network that is connected to the Internet.



## How you get your connection to the Internet



**FIGURE 4-1:** How you connect to the Internet.

In addition to connection services, most ISPs provide other services, such as

- » **Email addresses and message space on servers**

- » **Local news servers that replicate Usenet news groups**

These are discussion groups for various topics in a bulletin board format.

- » **Web page storage space**

There have been many technologies to connect to the Internet over the years beginning with dial-up access using the phone lines. Dial-up access to the Internet has given way to permanent connections, such as cable and ADSL (Asynchronous Digital Subscriber Line), which offer great improvements in access speed.

## *Working with an ASP*

*Application service providers* host servers for their clients. These servers may be database or mail servers, and may be shared or dedicated to a single customer. In either case, the server's hardware and software are maintained by someone other than the customer. This is a useful setup for smaller organizations because they do not have to invest in large servers or personnel to manage them. Rather, they basically rent space on them.



**REMEMBER** You will not be tested on ASP for the A+ exams. I include this information, though, because application service providers are sometimes considered to be a type of ISP, although they usually offer only data and content services and not connection services.

## *Understanding Internet Protocols*

When many people think of protocols and computers, network and transport protocols come to mind. These two types of protocols seem to get all the credit. Network and transport protocols are the network communications components that connect your computer to a network, sending and receiving bundles of data between hosts. TCP/IP is the main protocol found today on networks.

Generically, a *protocol* is a set of standards or conventions that are followed when formatting data to be used for electronic communications, and data transfer is just one level in the electronic communications model. This definition of protocol is not limited to data transfer, and a number of protocols work at other layers: most notably, the application layer.

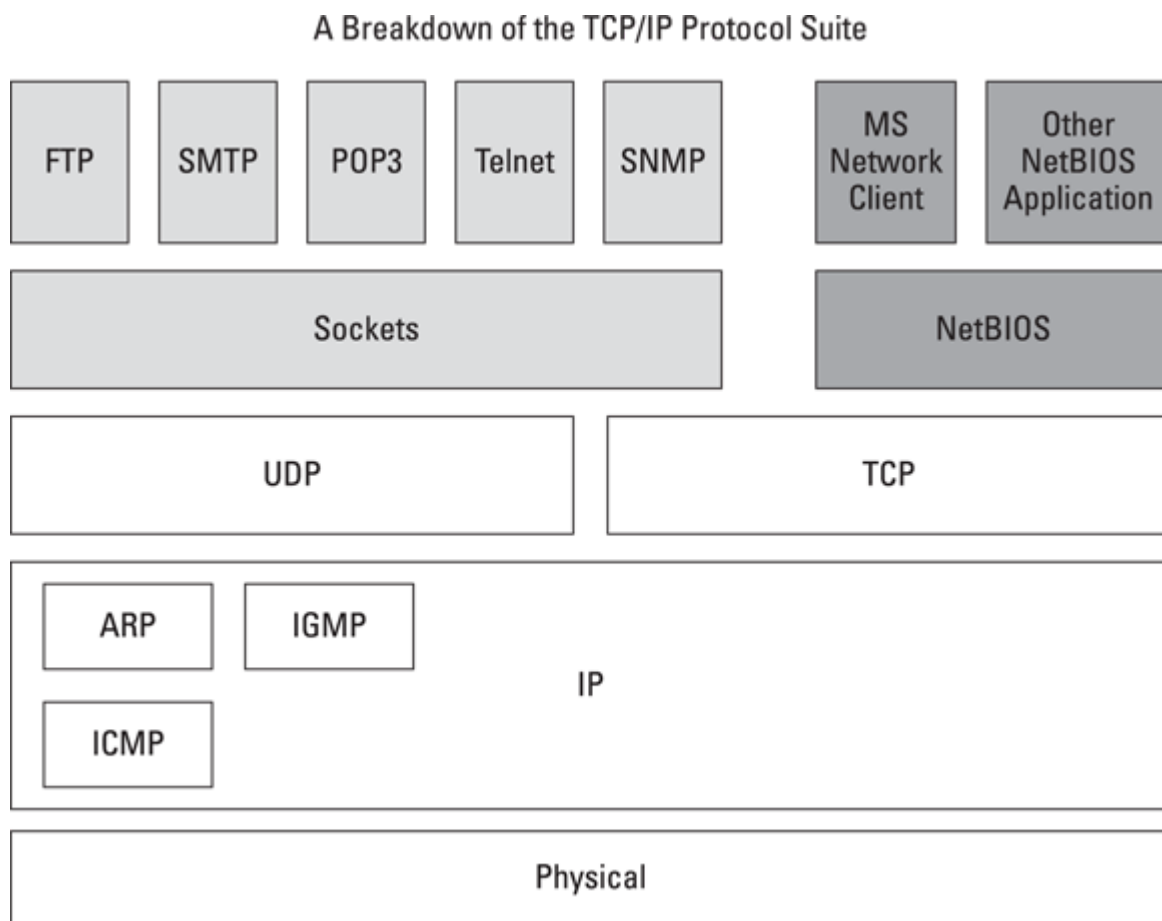
*Application layer protocols* establish a standard or format for data that is to be communicated. These protocols are so-named because they are the first layer to which programs or applications on a computer (as well as the server components) communicate.

### *TCP/IP*

TCP/IP is not a protocol in and of itself; rather, it is a suite of industry-standard protocols. It is a routable protocol that is used for

communication on the LAN or across networks. TCP/IP standards are developed, established, and used by the computing community itself.

[Figure 4-2](#) shows some protocols used as part of the TCP/IP protocol suite and what each protocol is responsible for. At the lowest level, IP offers best-effort delivery services. That is, IP attempts to deliver all network packets to the best of its ability. It also processes any errors reported back from routers. At the next level, TCP offers guaranteed delivery services, and UDP (User Datagram Protocol) offers best-effort delivery services.



**FIGURE 4-2:** TCP/IP uses many protocols at different layers to accomplish its task.

Session services for TCP/IP are offered by either NetBIOS over TCP/IP (NetBT) or Windows Sockets (Winsock). The NetBIOS session interface is used by all Microsoft network clients as their method of communicating with Microsoft servers on the network. The Winsock interface is

Microsoft's implementation of *BSD sockets*, which is the primary session interface that has been used on all UNIX and UNIX-based systems. Because most Internet servers originally ran UNIX, the application layer protocols (such as HTTP, FTP, SMTP, and POP3) are all designed to communicate through the socket-based session interface.

## *Email*

Email is one of the applications that made the Internet indispensable to most people. Email was an early tool for ARPANET that enabled users to communicate ideas and concepts to colleagues many miles away. Email allows for individually addressed text messages to be transferred over the Internet and delivered directly to the targeted recipient(s). Compared with conventional land-based mail (snail-mail), these transfers are instantaneous.

Attachments that accompany email messages are converted into a text stream by means of encoding. MIME (Multipurpose Internet Mail Extensions) is currently one of the most popular encoding methods on the Internet. Other popular encoding formats include BinHex and UUencode. *Encoding*, which converts binary data containing 8 bits per byte to ASCII or text data with 7 bits per byte, enables binary attachments to be sent over the text-based email network. When you receive attachments, they must be decoded by your email program. If your email program cannot do this, however, you have to use a third-party application to decode the files.

When it comes to reading your email, you can choose from a wide variety of applications. In fact, the list of clients is extensive, including command line clients, Windows-based clients, and web-based clients.



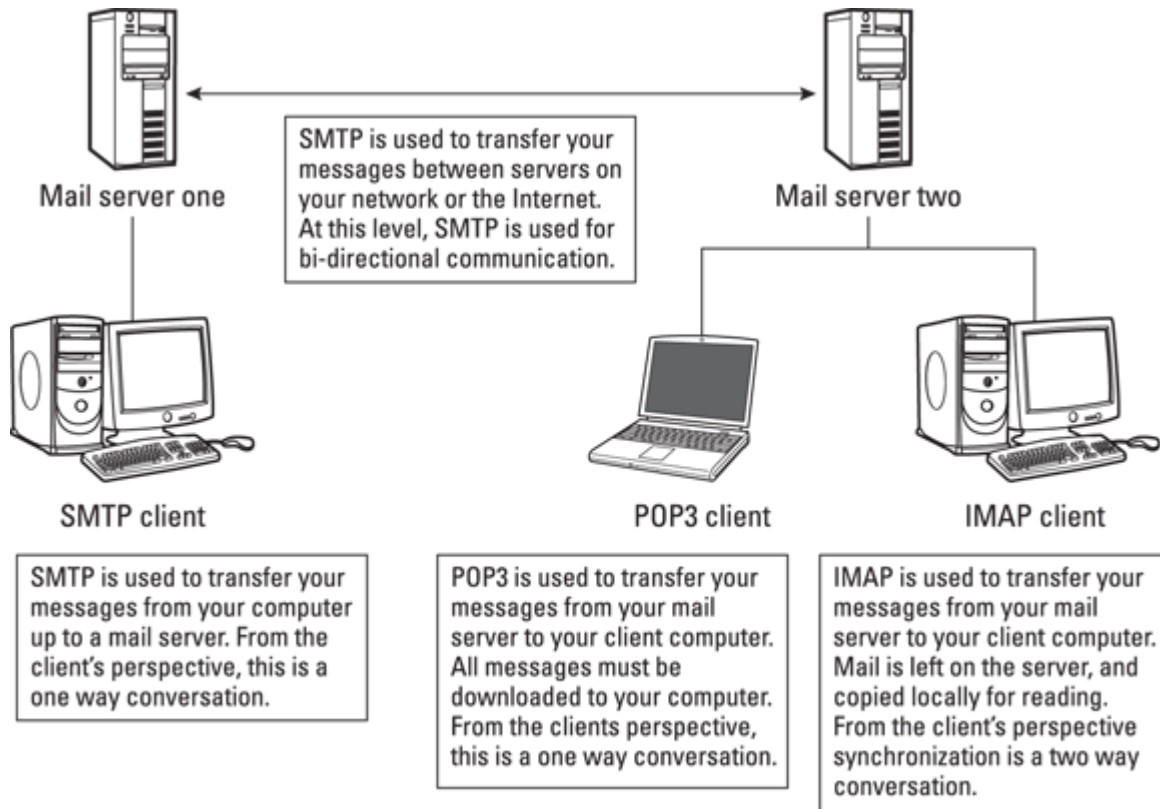
FOR THE  
EXAM

The three basic protocols used with email are *POP3*, *SMTP*, and *IMAP*:

» SMTP is the Internet protocol used to send email.

» POP3 and IMAP are the Internet protocols used to receive email.

Some email clients may support more than one access protocol. SMTP and POP3 are the most commonly used protocols although IMAP is increasing in popularity on private networks. [Figure 4-3](#) shows how these three protocols fit together, and the following sections discuss them in more detail.



**FIGURE 4-3:** Where mail protocols are used.

## **SMTP**

*Simple Mail Transport Protocol* (SMTP) is a mail delivery protocol, used to transfer mail messages from your mail client to a mail server. After the mail message is in the queue on the server, SMTP is also used to transfer the message to the mail server that is responsible for the target domain, such as @gleneclarke.com. The primary goal of SMTP is to get the mail messages to the server that hosts email for that domain.

## **POP3**

*Post Office Protocol version 3* (POP3) is a client access protocol, used to access or retrieve mail from a server. POP3 does not *send* email — that is the responsibility of the SMTP. When you configure your email client, you will configure it with the pair of servers: POP3 for downloading or reading, and SMTP for sending (see the preceding section). POP3 clients usually download all mail messages for their servers and delete the mail from the server. This action then leaves the mail only on the client computer.

## ***IMAP***

*Internet Message Access Protocol* (IMAP) is also a client access protocol for mail. As an IMAP client, you retrieve a list of messages that exist on the mail server and download only messages that you want to read. Any downloaded messages are also left on the server. Changes to your mail files locally can also be replicated to the server. Because you can download all messages, you can work entirely offline. If you delete messages while working offline, those deletions will be replicated to the server the next time you connect, in turn deleting the messages on the server.

## ***Configuring an email client***

When you want to read email, you must first configure an email program on your system. This email program is also known as an email client because it connects to the service provider's email server and downloads the email to your system using POP3 or IMAP.

There are a number of email programs you can use as a POP3 client and configure to connect to the ISP's email server. You can use the popular Microsoft Outlook, or use a free program such as Opera Mail.

To make this connection with an email client, you need the following information:

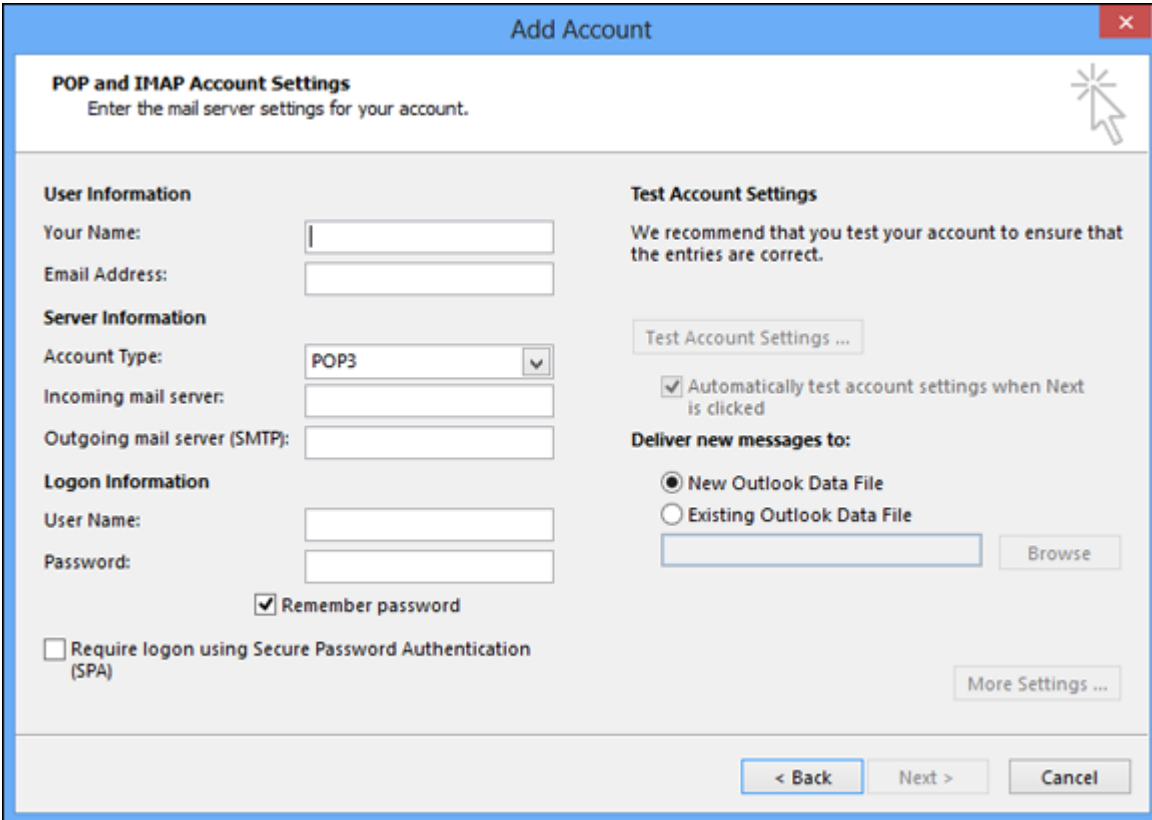
- » **Username:** The username is provided by the service provider and most times may be the first part of your email address. For example, the account [bobsmith@myisp.com](mailto:bobsmith@myisp.com) would most likely have a username of bobsmith.

- » **Password:** The password is supplied by the ISP when it created your account. Make sure that you change that password so that no one can easily guess the password.
- » **SMTP Server (outgoing server):** This is the address of the server that will send emails for you. You can input the IP address or the FQDN of the server, such as `mail.myisp.com` or `smtp.myisp.com`.
- » **POP3/IMAP Server (incoming server):** This is the address of the server that you download your emails from. It is most likely the same system as the SMTP server that sends your emails. Again, you can use the IP address or the FQDN of the server, such as `mail.myisp.com` or `smtp.myisp.com`.

The following steps demonstrate how to configure the Outlook 2016 client as a POP3 client:

1. **Launch Outlook by clicking the icon on the Taskbar and then choose Next on the Welcome to Outlook 2016 screen.**
2. **Choose Yes to set up Outlook to connect to an email account and then choose Next.**
3. **Choose Manual setup or additional server types in order to specify your POP3 and SMTP server settings along with your email account information.**
4. **Choose POP or IMAP as the service type and then choose Next.**
5. **Fill in your user information such as your name and email address.**
6. **In the Server Information area, specify whether you are using POP3 or IMAP to connect to the mail server and download the mail.**  
You will most likely use POP3.
7. **Type the address of your POP3 server (Incoming mail server) and SMTP server (Outgoing mail server), as shown in [Figure 4-4](#).**  
You are asked for your account name and password. You will need to get this information from the email provider.

8. In the Login Information section, provide your username and password and then select Remember Password.
9. Choose Next and then Finish.



**FIGURE 4-4:** Configuring SMTP and POP3 server settings.

When configuring email software, you may need to specify other configuration settings depending on the software you are configuring. Following are some common settings that may need to be configured:

- » **Port and SSL settings:** You may need to configure the email client port for nonsecure and secure (SSL) email:
  - For nonsecure email, the default port is 110 for POP3 and 143 for IMAP.
  - For secure (SSL) email access, the ports are 995 for secure POP3 over SSL and 993 for secure IMAP over SSL.



» **Exchange:** You may need to connect your email software to the company Exchange server. Microsoft Exchange Server is the name of the Microsoft mail server product that companies use to host their own email. To connect to the Exchange server from Outlook, you need to specify

- The name of the Exchange server
- The mailbox name you want to connect to

» **Gmail:** Many people are using online email providers such as Hotmail and Gmail to access their email over HTTP. You can configure most email software to connect to the Hotmail or Gmail mailboxes by just typing in the email address of the account.



TECHNICAL  
STUFF

Web mail accounts, such as Hotmail and Gmail, have become increasingly popular over using POP3 and IMAP. These accounts leave their mail messages on the server in a manner similar to IMAP.

## *Hypertext Transport Protocol*

Much older than the Internet, the concept of hypertext has been around since 1945 when Vannevar Bush wrote an article titled “As We May Think.” The word *hypertext* was coined in 1965 by Ted Nelson.

Hypertext was a means of indexing, or cross-referencing, data found in different documents, allowing users to quickly move to linked documents.

## **HYPERTEXT IN ACTION: HYPERCARD**

One commercial implementation of hypertext was the Apple Macintosh program HyperCard (released in 1987). HyperCard was a kind of stack of virtual index cards, each holding common GUI items, such as text boxes, graphics, or buttons.

These cards could be reviewed in order, or links could be made to allow for hypertext navigation through the stack. This feature allowed the HyperCard to be used for presentations, games, and a variety of other functions.

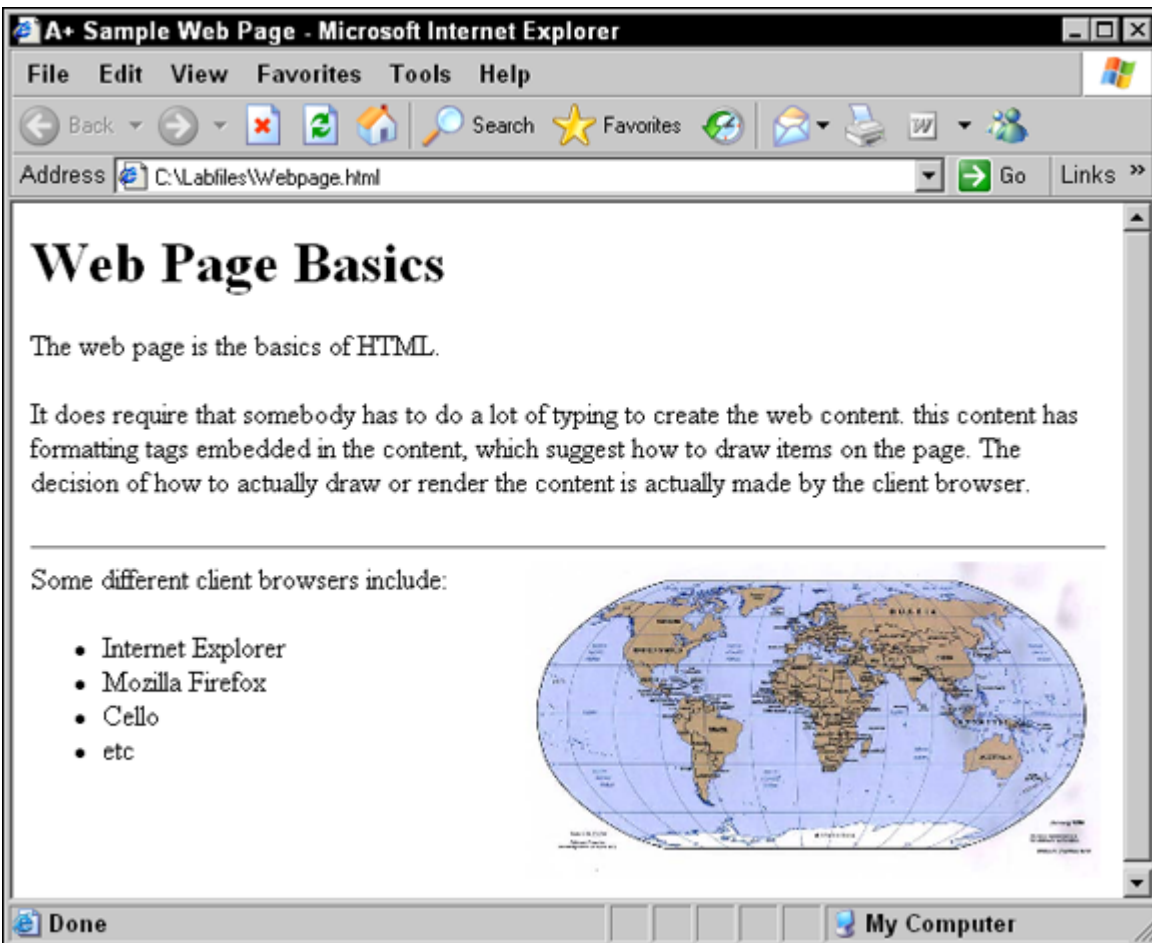
In the early days of the Internet, you could transfer data as files between computers. After being uploaded to the server by the data owner, these files were available for download from those servers, which meant you had to know what files you needed and what servers they came from. Your text files, formatted documents, and graphics could be transferred between computers. After you downloaded the files, they could be opened and viewed, but there was no way to view them in an attractively formatted style in the online environment, especially in a format that was universally accessible. Most formatted documents were created and formatted in proprietary programs like Microsoft Word or Adobe PageMaker — and thus readable only by people who have those programs.

To address the problem of knowing which servers you were accessing data from, Paul Lindner and Mark McCahill (University of Minnesota) came up with an idea that became the Gopher protocol in 1991. Gopher used hypertext concepts and allowed you to place a pointer on your server that would connect people to specific directories on other servers elsewhere on the Internet. This made browsing information scattered across servers very easy because switching between servers became completely transparent. Gopher became the most popular tool for downloading files and data from the Internet.

At the same time Gopher was being developed, the researcher Tim Berners-Lee at CERN was working on a hypertext system he called World Wide Web (choosing that name over The Information Mesh). This system implemented a protocol called HTTP, which allowed for transparent linking of documents between servers. This capability was possibly thanks to the new Hypertext Markup Language (HTML) that was being used for World Wide Web data.

The tool that accesses HTTP servers and HTML files is, of course, the web browser. A web browser retrieves the files from the server, displays the formatted document, and links to other servers as required. Early web browsers displayed text and images as separate but linked documents, so you could view images if you followed an image link. The web really took off in 1993 when Marc Andreessen of the National Center for

Supercomputing Applications (NCSA) released NCSA Mosaic and offered something the Gopher and other web browsers lacked — the capability to view text and graphics mixed together in a single frame. Internet users flocked to this new technology that gave their data the same appearance as the paper-bound copies. [Figure 4-5](#) shows a formatted document in a web browser.



**FIGURE 4-5:** Web browsers let you retrieve data from a server using HTTP.

## ***Hypertext Markup Language***

*Hypertext Markup Language* (HTML) is a form of SGML that offers a universal way to format documents. Standards for SGML are more complex than for HTML. SGML is actually a method of creating interchangeable, structured documents so that they can be universally accessed from different types of systems. SGML can take data from a variety of sources (such as word processors and graphics applications)

and join them as a single structured document by using Document Type Definitions (DTDs). Different DTDs are identified in a document with the aid of markups or tags, which show or identify the divisions or sections.

HTML is actually just a DTD that is one of the many small parts of SGML. With the simple initial requirements for formatting of documents, Tim Berners-Lee decided that keeping the formatting language simple was the best course of action for the web, so HTML was adopted in favor of SGML.

HTML files are text or ASCII files, but they contain formatting codes that are embedded in the text. The web, or HTML, page displayed in [Figure 4-5](#) was generated with the following script ([Listing 4-1](#)).

### **LISTING 4-1 Script Used to Create the Web Page Shown in [Figure 4-5](#)**

---

```
<html>
<head><title>A+ Sample Web Page</title> </head>
<body>
<h1>Web Page Basics</h1>
<p>The web page is the basics of HTML.</p>
<p>&lt;p&gt;It does require that somebody has to do a lot of typing to create the
web content. This content has formatting tags embedded in the content, which
suggest how to draw items on the <!--<ce:anchor id="pp:1029 np:1030"
role="page-break"/>-->page. The decision of how to actually draw or render
the content is actually made by the client browser.&lt;/p&gt;
<hr>

Some different client browsers include:
<ul>
<li>Internet Explorer
<li>Mozilla Firefox
<li>Cello
<li>etc
</ul>
</body>
</html>
```

Early HTML files were saved with either the .html or .htm extension, but now may have a variety of extensions (such as .php or .asp) because

of various scripting languages being used to build dynamic web pages.

HTML has gone through many revisions; the last revision was version 5. Changes are being made to HTML with the integration of XML (Extensible Markup Language). XML, which adds functionality to support database data exchange, is designed to transfer not only sections of data from a database but also its structure. XML has become very popular and is a huge Internet buzzword.

As I mention, XML has been rolled into the HTML standard, forming the XHTML (Extensible Hypertext Markup Language) standard, so HTML is now XHTML. The current version of XHTML is 1.0, with 2.0 just around the corner with a working draft already in place. For more information about XML, HTML, and XHTML standards, visit the World Wide Web Consortium at [www.w3.org](http://www.w3.org).

## ***HTTPS and SSL***

*HTTPS* is a secure version of the Hypertext Transport Protocol. When you use HTTP, all communication between you and the server is in cleartext, so anyone can easily read all that communication. HTTPS uses SSL (Secure Sockets Layer) or its successor, TLS (Transport Layer Security), to provide authentication and encryption services.



**REMEMBER** HTTP communicates with a server on TCP port 80, and HTTPS uses TCP port 443.

To implement SSL, a web server needs to have a security certificate installed to verify its identity for you. When you are confident that the server is who it says it is, you can then carry out secure and encrypted data transfers with it.

Early SSL used 40-bit encryption keys, which were not secure and were easy to break. Current SSL uses 128-bit or larger keys and is very hard to break, making data protected with SSL very secure.



FOR THE  
EXAM

Do not confuse the flurry of H-based acronyms used for the World Wide Web. HTML is the document formatting; HTTP is the cleartext transfer protocol that uses TCP port 80; and HTTPS is an encrypted transfer protocol — secured by SSL or TLS — which uses TCP port 443.

## *File Transfer Protocol*

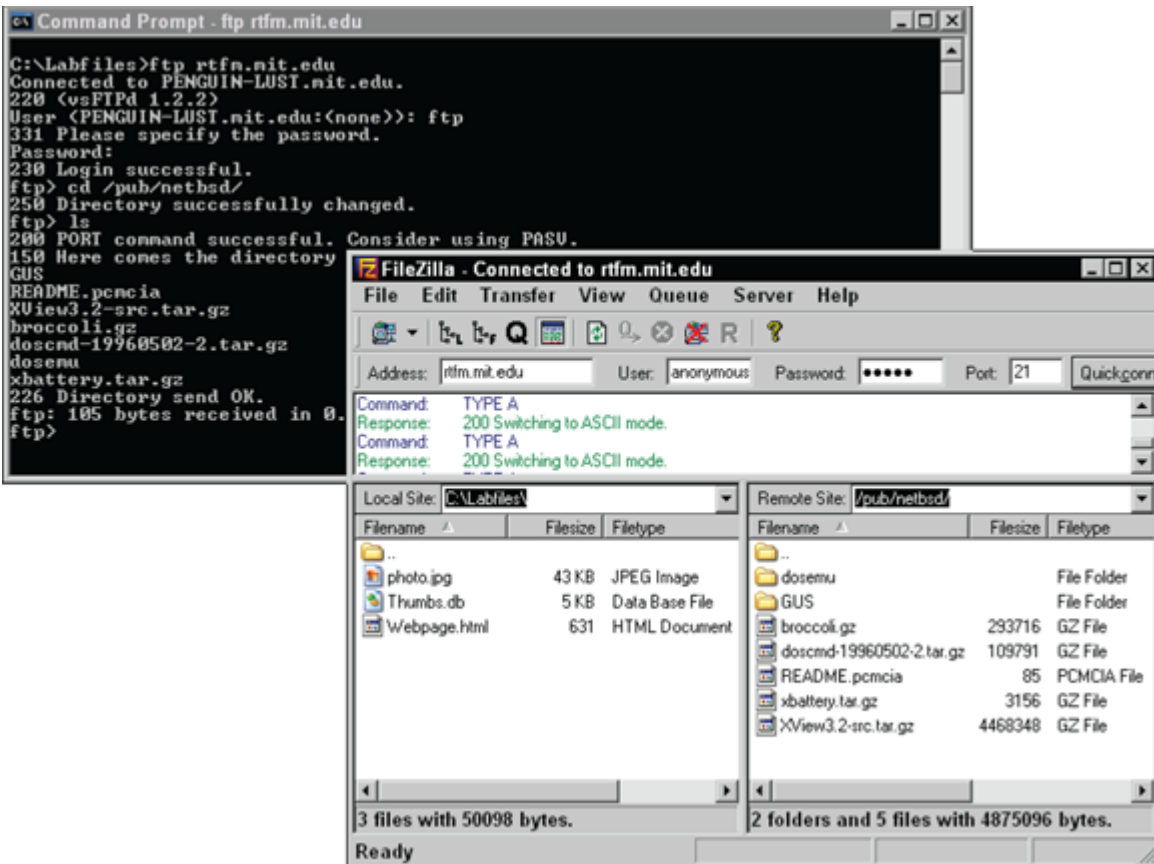
The first scientists using the Internet established early during the evolution of the Internet that there would have to be some format to allow for the transfer of data (as opposed to text messages) across the Internet. The solution was File Transfer Protocol (FTP), which allows files to be uploaded and downloaded from servers. FTP requires an accessible directory or folder, a server-side service (or *daemon*), and a client.

### DAEMONS

A *Windows service* is an application that runs without a user interface and without anyone being logged onto the computer. This background application provides functions to the local computer or to remote users.

These functions include items such as file- and printer-sharing, messaging, and publishing web pages. Linux and Unix servers call these background services *daemons*.

There are a large number of FTP clients to choose from, ranging from command line–based to graphical (like FileZilla or WinSCP). [Figure 4-6](#) shows some different FTP clients available on the Windows platform. If you regularly work with FTP, then you will likely want to learn one of these clients, rather than relying on the FTP features that are included with most web browsers.



**FIGURE 4-6:** Choosing the right client for the job is important.

Because of the method that traditional FTP servers used, they were not Network Address Translation (NAT) friendly when the server was placed behind a NAT gateway or firewall. That led to the creation of passive FTP, which changes the orientation of connections in the FTP process. To make use of a passive FTP server, your FTP client has to support and be configured to use passive FTP.

Because the FTP authentication and data-transfer process is all in cleartext or unencrypted data packets, a new protocol has been created — Secure Copy Protocol (SCP) — which transfers files over `ssh` (covered later in this chapter) on TCP port 22. SCP has been replaced for most people with Secure File Transfer Protocol (SFTP), which also uses `ssh` and is a more feature-rich protocol.

## *Command shells*

A *shell* is an interface for users to connect to. When you log onto your Windows computer, your desktop environment is generated by `explorer.exe`. On Unix and Linux servers, if administrators choose not to load a graphical environment, the shell application would be command line driven, usually with some variant of `bash` (Bourne-Again Shell). Because most Unix or Linux server administration can be done from the command line, remote shell access to a server is very important, both from the aspect of remote administration and for security. In addition to these servers, many network devices (such as routers, switches, and hardware firewalls) support a remote management command shell. The two most common methods of connecting to these command shells are `telnet` and `ssh`.



TECHNICAL  
STUFF

Windows Server 2008 has an installation method called Server Core Installation that does not install the default GUI (`explorer.exe`) but rather allows all administration to be performed via a command prompt or using GUI tools remotely. This type of installation reduces maintenance, the attack surface, and management, and also uses less disk space.

### *telnet*

`telnet`, developed in 1969, has been the long-standing standard for remote management, in spite of its long-standing security flaw. The largest single flaw with `telnet` is that the entire communication process between the client and server takes place in cleartext. For any person in a position to view the raw network traffic, the entire conversation can be viewed, including the logon usernames and passwords. Server administrators moved to newer management technology some time ago, but many hardware manufacturers kept using `telnet` until fairly recently. Windows includes a default command line `telnet` application, and you can also get third-party graphical `telnet` applications that allow you to easily manage multiple sessions or capture log files of sessions.

### *ssh*



`ssh`, developed in 1995, is short for *secure shell*. Remote access to a shell on a computer is what `ssh` is designed to secure, just like the name suggests. In addition to allowing remote shell access to servers, `ssh` allows for opening secure tunnels, allowing secure access to other systems on a remote network through the tunnel. When working with `ssh` with the lowest security level, the server uses a certificate to generate initial encryption keys and then encrypt the data stream between the client and server. For stronger security, client certificates can be used for authentication of the client as well as the server using its certificate. Server administrators that dealt with `telnet` cleartext data for years quickly converted to `ssh` when it became available, making it the new standard in remote shell access. Some `telnet` holdouts, like network switch manufacturers, have finally listened to their customers and added support for `ssh`. It is now prevalent on all systems that traditionally supported `telnet`. In order to use `ssh`, you will require a client, such as PuTTY ([www.chiark.greenend.org.uk/~sgtatham/putty](http://www.chiark.greenend.org.uk/~sgtatham/putty)).



**WARNING** `ssh` should be considered the minimum connection mechanism for remote devices. `telnet`, with its cleartext data transfers, should no longer be considered.

## *Installing and Configuring Browsers*

Internet Explorer (IE) is the default web browser for most Windows computers, partly because it comes installed with that OS. With this boost, Microsoft won the browser wars of the 1990s, which saw the main battle between IE and Netscape Navigator (even though both owed their roots to NCSA Mosaic). Although many different browsers were available in the beginning, these two products quickly rose to the top of the pile and battled it out. Today, there are different players in the game and there are

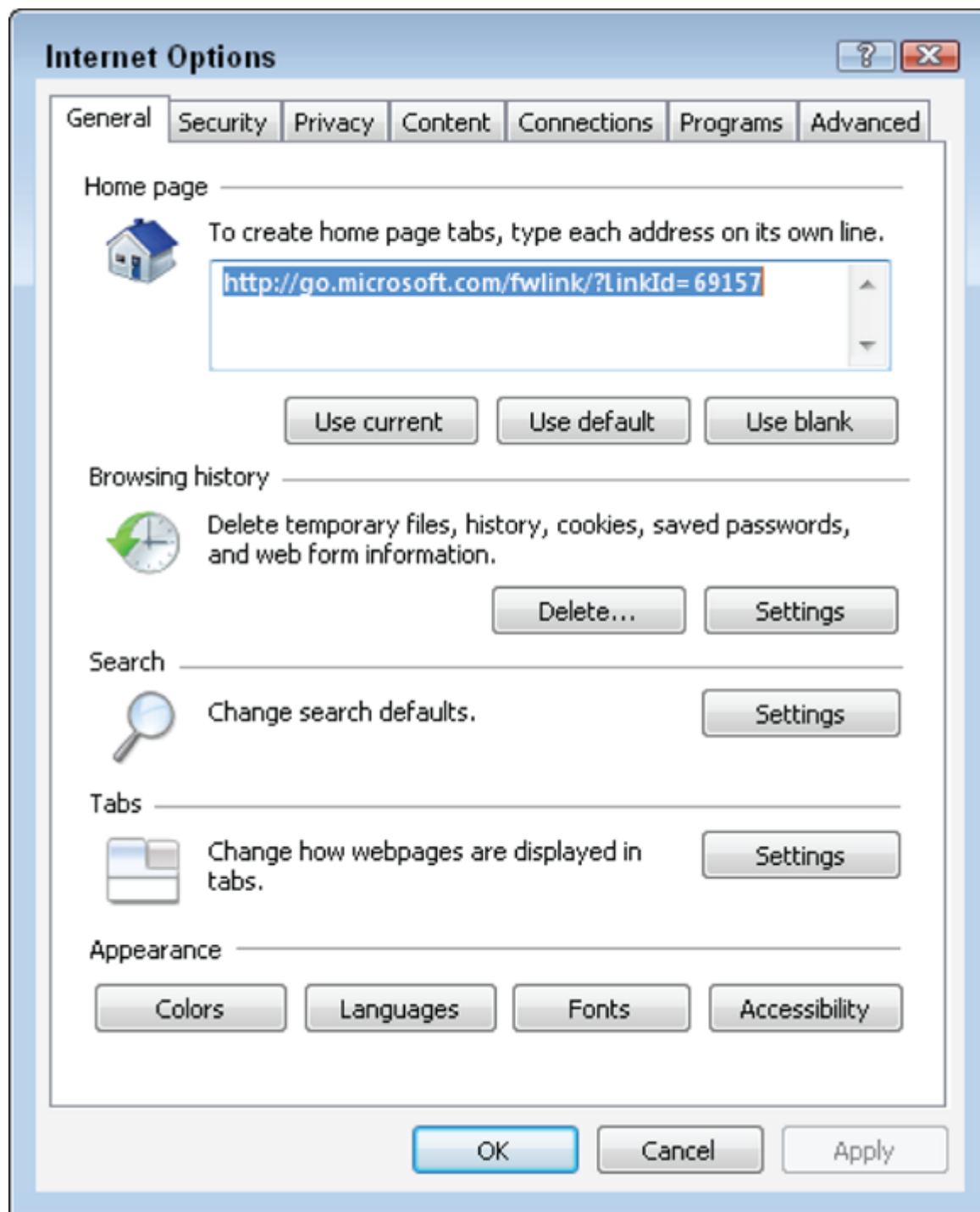
a number of other browsers that can be downloaded and installed onto your system, such as Firefox, Opera, and Google Chrome.

The browsers today are fairly comparable and have similar features, such as pop-up blockers and tabbed browsing, plus the ability to choose from thousands of add-ons (extensions) written to enhance the web browser.

The following sections look at Internet Explorer, although similar settings are available in most web browsers.



**REMEMBER** To configure IE settings, open IE and choose Tools (the gear icon in the top-right corner) ⇒ Internet Options, which opens the Internet Options dialog box shown in [Figure 4-7](#). This dialog box contains seven tabs, and I discuss each in the following sections.



**FIGURE 4-7:** Manage web browser settings through Internet Options.

## *Configuring General settings*

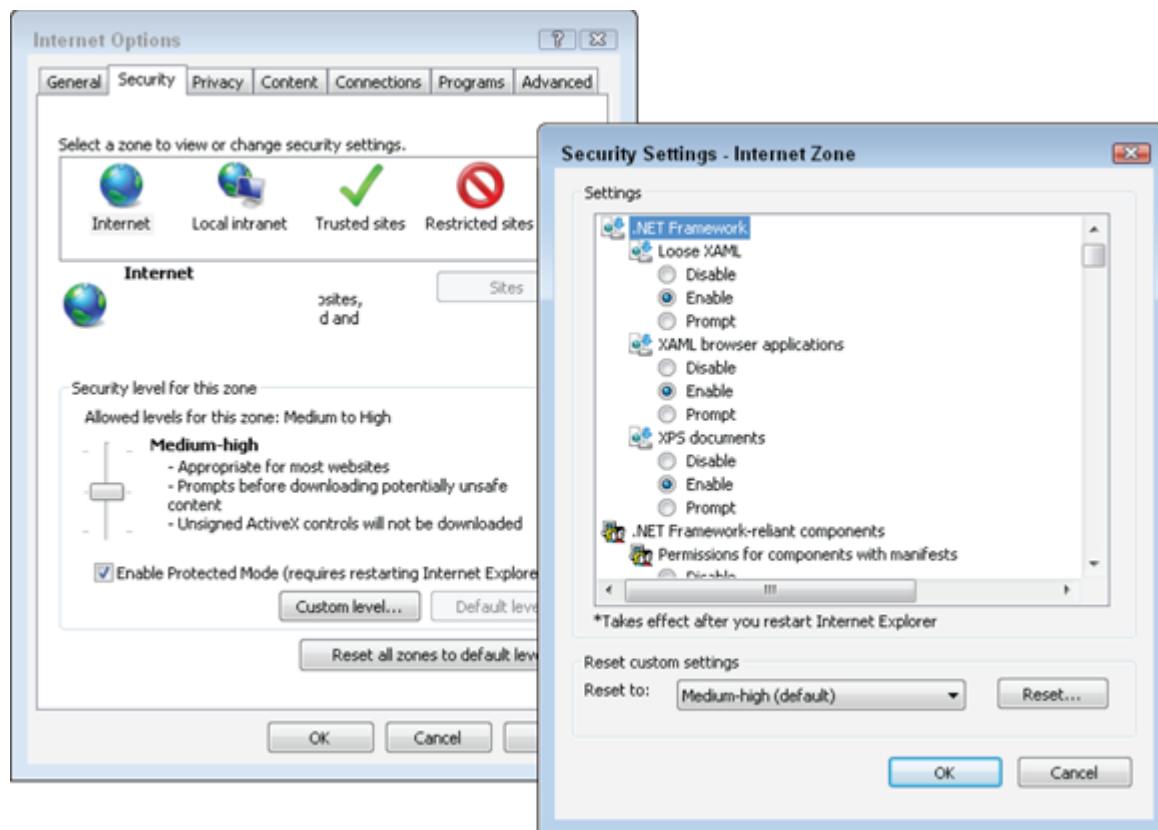
From the General tab (shown in [Figure 4-7](#)), you configure settings for your home page, browsing history (including temporary Internet files),

search defaults, and tabbed browsing. The other settings are primarily cosmetic. The settings for temporary Internet files allow you to choose the location of the files, how much space they will take on your hard drive, and your setting for refreshing content from the website directly.

## *Configuring Security settings*

From the Security tab, you set security settings for sites in one of four zones. Most sites that you visit will fall into the Internet Zone, and the Local Intranet, Trusted Sites, and Restricted Sites affect only sites that you specifically enter onto those lists. Each zone can have different security settings. And, for each zone, you can choose from one of five security levels or specify your own custom settings. The five built-in levels are High, Medium-High, Medium, Medium-Low, and Low, although for the Internet setting, you can choose from only the three highest settings.

Click the Custom Level button to see exactly what settings are enabled. The settings in the resultant dialog box, also shown in [Figure 4-8](#), allow you to set IE to handle a variety of components that may be embedded in web pages. For example, you can have IE disable, enable, or prompt you when it encounters certain components on websites, such as .NET Framework–reliant components, ActiveX controls and plug-ins, downloads (for files and fonts), scripting (including ActiveX scripting and Java applets), user authentication (often done automatically in the background), and a slew of user interface options.



**FIGURE 4-8:** Security settings in Internet Explorer can make the browser much safer.

## *Configuring Privacy settings*

The IE Privacy tab, which deals with cookies and pop-ups, works in a similar fashion to the Security tab. Here, you can configure settings for cookies on a per-site basis as well as configuring general settings by using either the slider for levels from Allow All Cookies to Block All Cookies (with four levels in between) or by clicking the Advanced button and then customizing your cookie settings.

*Cookies* are settings that are stored on your computer by your web browser. When you return to the web server later, these settings are sent back to a web server. Websites use cookies to track users, especially if the site uses a shopping cart–transaction system. Shopping carts allow you to browse a catalog, select items you want, and check out. This mechanism is not only used at shopping sites but also at download sites, where you can select multiple files and download them all in one action at the end of your visit.

In addition to shopping carts, many sites will store a unique ID in a cookie on your computer to track your return to the site. In some cases, the IDs are used to set user preference or to track unique visitors. Cookies are stored in text files on your system and generally use very little space. When visiting one website, you might see content that comes from another web server, which is the case with most of the banner ads that appear on websites. If this other web server attempts to have a cookie stored, it is called a third-party cookie. You might want to block third-party cookies or all cookies if you are concerned about having companies track your activity on their websites.

If you choose to block pop-ups, click the Settings button to configure settings as well as a list of sites that are allowed to use pop-ups.

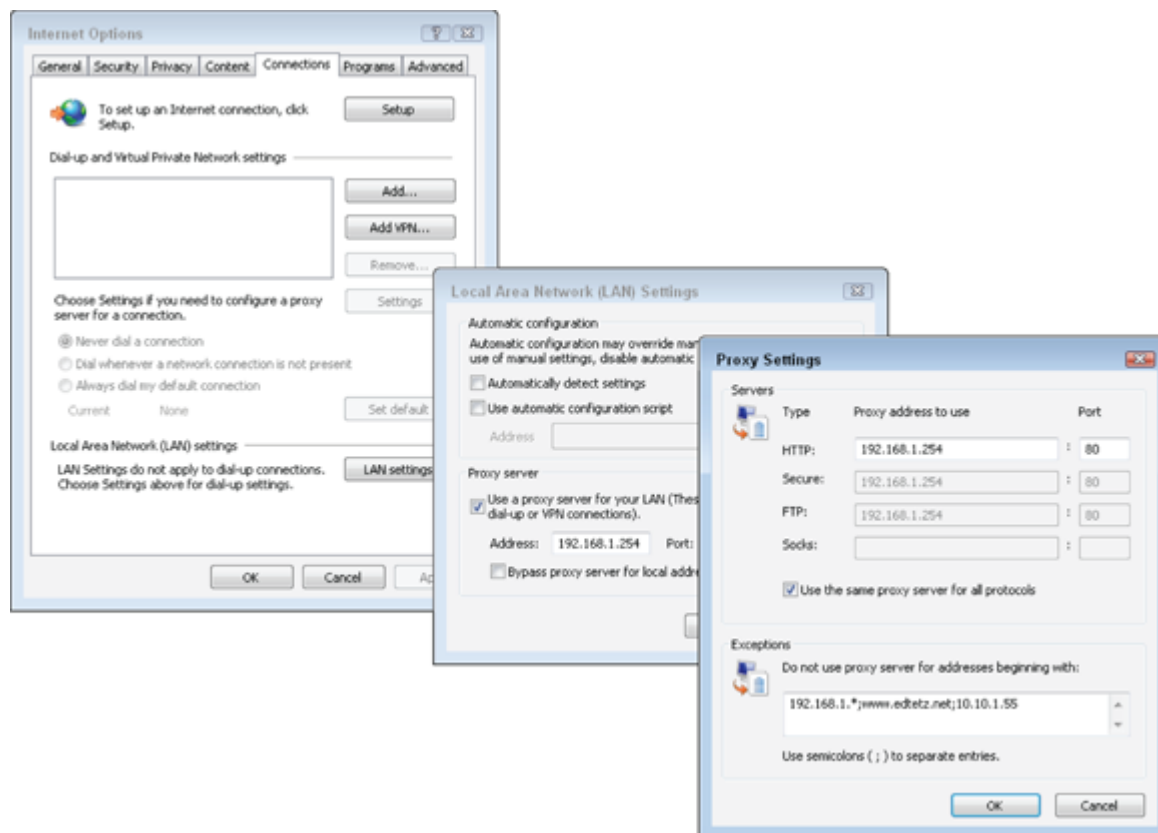
### *Configuring Content settings*

From the Content tab, you can enable the Content Advisor, which makes use of voluntary tags that web content developers can include on web pages. These tags rate the level of language, nudity, sex, and violence found on the page. With the Content Advisor enabled, you can block content that is above the customized configured level. The Certificates section allows you view and modify (import and export) SSL certificates that IE uses. The Personal Information section allows you to modify the AutoComplete settings that are used on forms you encounter on websites.

### *Configuring Connections settings*

A proxy server acts as a middleman when you request information from the Internet, allowing network administrators to restrict access through the network firewall, as well as audit what websites network users are going to. If you need to use a proxy server to browse the Internet, you can use the proxy settings to configure your access to proxy servers.

Proxy settings, found on the Connections tab, can be configured for each of the dial-up settings individually or for your LAN connection. Both have similar settings, so I discuss the LAN settings, which you reach by clicking the LAN Settings button. The settings are shown in [Figure 4-9](#) and include automatic proxy detection and configuration, which requires specific configuration settings on your network.



**FIGURE 4-9:** If you are using proxy settings, you might need to regularly enable or disable the settings.

In addition to this setting, you can manually configure a proxy server address and port for your particular network and use that same server for `http`, `https`, `ftp`, `gopher`, and `socks`. The `socks` setting allows you to proxy protocols other than the default ones that are listed. You might use `socks` to proxy IRC or POP3. As with most cases, you can also configure a list of servers that are exceptions to using the proxy server, which might be the case when you have servers on your internal network that you don't want to use a proxy server for.

## *Configuring Programs settings*

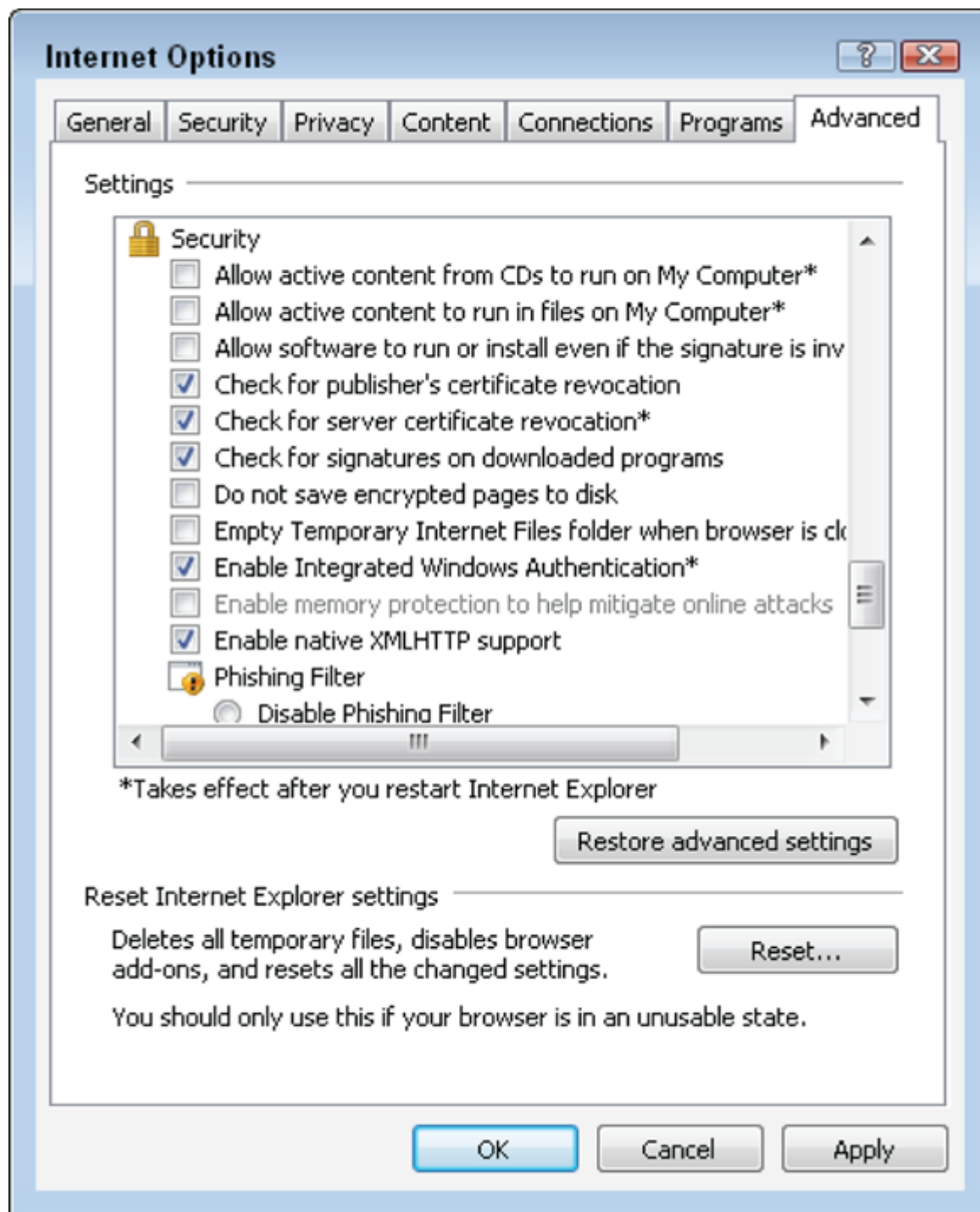
From the Programs tab, you can specify which programs to use for different types of Internet services, such as HTML editing, email, and newsgroups. In addition, you can configure and manage *IE add-ons*, which are third-party components loaded automatically by IE. The add-ons section is where you will find any additional programs and toolbars that may have been loaded on your system. Having many of these items

can slow down your system, so you may want to go into the add-ons and remove additional toolbars and extensions.

### ***Working with Advanced settings***

The last tab in Internet Explorer's Internet Options dialog box is the Advanced tab. It has a variety of settings you can modify (by enabling or disabling features and functions) how IE works. These settings are Accessibility, Browsing, HTTP 1.1, Java, Multimedia, Printing, and Security. See [Figure 4-10](#).





**FIGURE 4-10:** Security Settings are just one of the types of Advanced Settings.

## *Using the Internet*

When using the Internet, be aware where you are going when you click links on your web browser. This section looks at what makes up the parts of a *URL* (Uniform Resource Locator), the string of text that appears on the address line in IE. The standard URL has an access method, a server name, and the path to a file or directory on the server. A typical URL resembles the following:

```
http://www.glenecclarke.com/sample_files/default.htm
```

In this example, `http:` represents the access method, `//www.glenecclarke.com` represents the name of the server being contacted, `/sample_files` represents the directory being navigated to, and `/default.htm` represents the file being requested. All URLs follow the same basic structure, but if you leave out one part of it — such as the document name — you will be given the default document for that directory or server.

## *Access methods*

[Table 4-1](#) summarizes some of the access methods for resources on the Internet. These access methods can be specified from the command line or from within a web browser.

**TABLE 4-1 Access Methods**

<b>Access Method</b>	<b>Description</b>
<code>http:</code>	Used to access web content on servers
<code>https:</code>	Used to secure <code>http:</code> access, using SSL to provide authentication and encryption services <code>https:</code> requires a certificate to provide verification of the server's identity
<code>ftp:</code>	Used to copy files to and from remote servers
<code>mailto:</code>	Activates the local email client to send a message to the address specified in the server portion of the URL

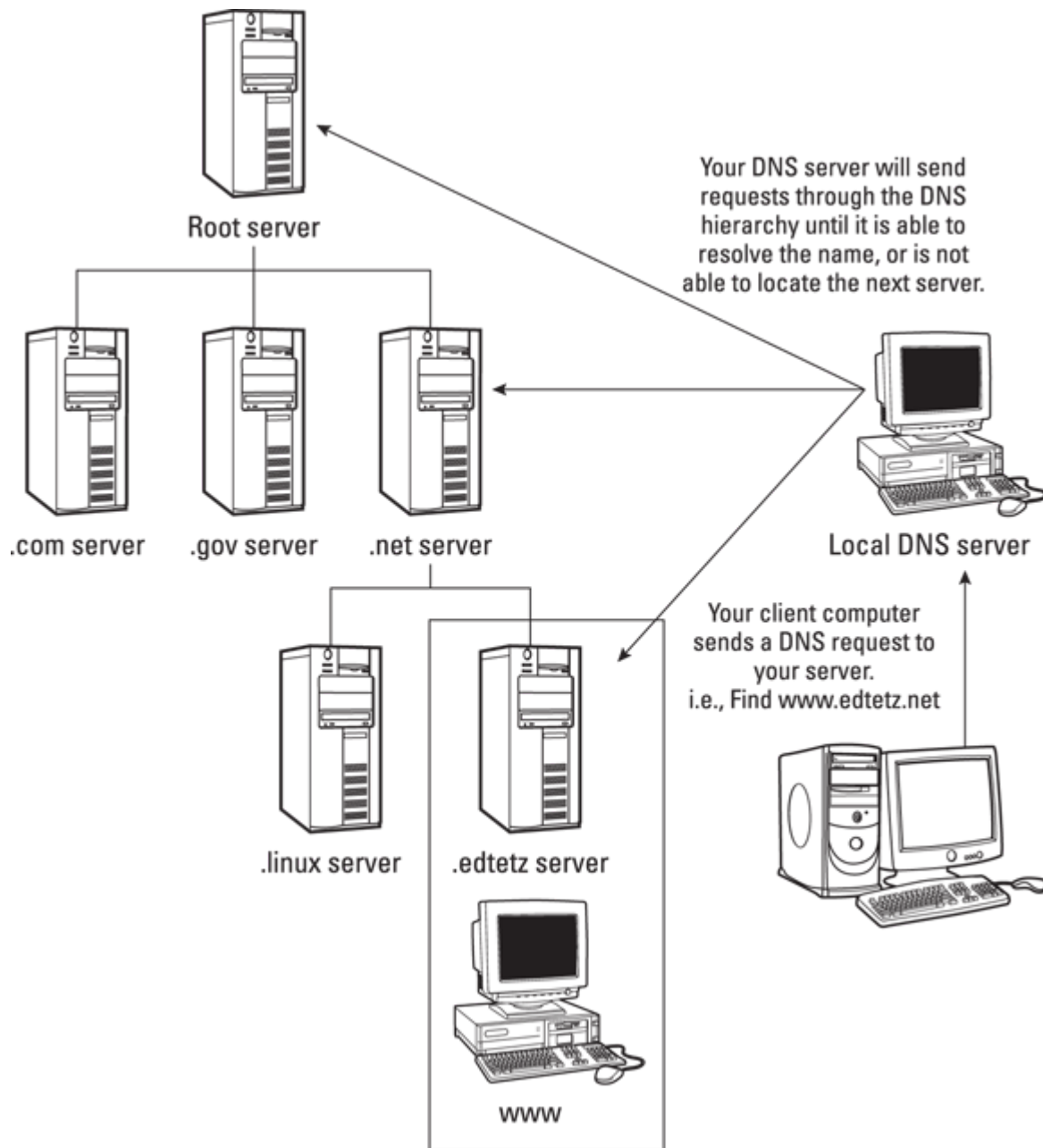
## *Domain names and websites*

Every computer on the Internet has a unique IP address. This address enables a computer to find and establish communications sessions with

any other computer — that is, as long as you know the IP address of the computer you want to connect to.

Every IP address is potentially a 12-digit number. Because every IP address could be a 12-digit number — and because most people cannot remember hundreds of 12-digit numbers — the domain name system (DNS) was established in 1984. With DNS, you specify a name, and the DNS resolver or client on your computer will look up the required address for you on a DNS server.

Because each server could never be able to hold the names of all the computers on the Internet, DNS servers split up the job. Each server is responsible for knowing only a small number of computers, but the servers know how to find other servers. [Figure 4-11](#) illustrates how the DNS is structured. At the top of the structure is the root (.) domain, which knows about all the servers that manage the top-level domains (TLDs). TLDs include `com` (commercial), `org` (organization), `mil` (military), `edu` (education), `gov` (government), and `net` (network), as well as a two-letter domain for every country in the world, such as `au` (Australia), `us` (United States), `uk` (United Kingdom), and `de` (Germany). The servers at the top level know about the servers that are responsible for the next level down, and so on.



**FIGURE 4-11:** Overview of the domain name system.



TECHNICAL  
STUFF

Restrictions around top-level domains have become more relaxed. As such, the Internet Corporation for Assigned Names and Numbers (ICANN) has registered several new TLDs, such as `travel` (travel industry), `name` (personal names), `museum`

(museums), `mobi` (mobile products and services), `jobs` (HR related), `info` (informative websites), and `aero` (air transportation and aerospace; maintained by Internet Assigned Numbers Authority [IANA]). There are also misused TLDs, such as `ws` (officially for the country of Western Samoa, but often used for personal websites) and `tv` (officially for the country of Tuvalu, but often used for television-related sites).



FOR THE  
EXAM

DNS is a global directory that allows friendly names to be resolved to IP addresses. Without this function being performed, you would have to know every server's IP address.

Here's how it all works in real life. Say you want to connect to a server with a DNS name of [www.glenecclarke.com](http://www.glenecclarke.com). Your DNS client checks against your local server to see whether it knows the IP address for that DNS name. Even if your server is not the owner of that DNS name, it may have looked it up before and have the information cached. If the information is not cached on the local server, your server forwards the request to one of the root-level servers, which directs it to the `.com` server, which directs it to the `glenecclarke` server, which then looks up the `www` record.

This system gives your browser the capability of finding any computer on the Internet with a name registered with DNS. Many people register their servers by the type of service that they offer, such as

`ftp.glenecclarke.com`, `smtp.glenecclarke.com`, `pop3.glenecclarke.com`, or `mail.glenecclarke.com`. HTTP allows you to place links on any server to any other server on the Internet, which allows you to have a very complex path configured to lead people through the Internet. Because this path is web-like, the interconnection of HTTP servers is referred to as the *World Wide Web* (`www`). `www` is the standard name that is given to the HTTP or web servers on the Internet.

When you connect to a server, the URL might have a path listed beyond the root directory, or it might have the complete path to a file on the

server. If no filename is given, the web server usually displays a default document for that directory, such as `default.htm` or `index.htm`. If no default document exists for that directory and the server allows for viewing the directory listing, you will see a list of filenames found in the directory, with each filename being a link to the file. When no other condition is met, the server returns a `not found` or `404 error` message.

## *Ways to Access the Internet*

In addition to dial-up connections, many other types of connections can connect you to the Internet, and some of these connection types might be available in your area from local Internet service providers (ISPs). Some of these are used for home connections, and others are used primarily for connecting LANs to the Internet:

- » Dial-up
- » Cable
- » DSL
- » ISDN
- » T1/T3
- » Fiber
- » Satellite
- » Wireless
- » Line-of-sight wireless Internet service
- » Cellular (mobile hotspot)
- » WiMax

The following sections take a closer look at each of these Internet connection types.

### *Dial-up*

Good-old reliable dial-up has remained a true friend of remote access and access to the Internet for years. For years, dial-up was the method available to most users, and dial-up access was much better than no access. Dial-up is still a standard way to connect to the Internet in many markets in which faster alternatives do not exist. The listed data rate for dial-up connections is 56 Kbps.

## *Cable*

Cable connections implement a cable modem in your home or office that takes a digital network signal from your network card and translates (modulates) it into an analog broadband signal. This signal is then passed on to the cable network. Cable companies usually offer transmission speeds between 4 and 30 Mbps to their customers although actual speeds vary. This signal runs over existing cable, using previously unused signal areas of the medium. When using cable, you are on a shared medium with other users until your connection reaches the cable company's office.

## *DSL*

The most common form of Digital Subscriber Line (DSL) is *Asynchronous Digital Subscriber Line* (ADSL). An ADSL implementation works similarly to cable (see the preceding section) except that the device you have in your home or office takes the digital signal from your network card and passes it to a phone line. ADSL companies usually offer transmission speeds between 4 and 8 Mbps, although actual speeds vary. Cable offers the same transmission speeds going to and from the Internet, but ADSL always has slower upload speeds because the connection is broken into upstream and downstream channels. With ADSL, surfing the Internet and copying large files from websites is very fast, but if you want to store a file on a website or send email with large attachments, your speeds will be substantially slower. Typical upload speeds for ADSL range between 64 Kbps and 1 Mbps.

The standards for ADSL2 and ADSL2+ have been released, so some vendors may choose to implement these versions of ADSL, allowing for download speeds from 5 to 12 Mbps for ADSL2 and up to 24 Mbps for ADSL2+, although both offer upload speeds only in the 1–3.5 Mbps

range. With ADSL, you share the line only until you hit the Telco switching office, which typically must be closer than 3 miles (5 kilometers).



FOR THE  
EXAM

Broadband, high-speed Internet connections through cable, and DSL (of which ADSL is a subtype) have replaced dial-up in most regions.

## ***ISDN***

Integrated Services Digital Network (ISDN) service comes in two basic forms: basic rate and primary rate.

- » **Basic-rate ISDN:** Uses three channels: two 64 Kbps lines for data (128 Kbps) and one 16 Kbps line as a control channel, which is used for establishing and maintaining connections. The data channels are referred to as B channels, and the control channel is referred to as a D channel.
- » **Primary-rate ISDN:** Uses twenty-three 64 Kbps B data channels (1.44 Mbps) and one 64 Kbps D channel for control information.

## ***T1/T3***

T1 connections offer transmission speeds of 1.544 Mbps over 24 pairs of wires. Each pair of wires can carry a 64 Kbps signal, called a *channel*. T1 connections can be implemented over copper wire.

T3 connections, on the other hand, require a better medium than copper, such as microwave or fiber optic. They are capable of speeds ranging from 6 Mbps to 45 Mbps.

T1 and T3 are North American standards, and E1 and E3 are similar standards for the European community.

## ***Fiber***



Internet access over fiber connections is defined in the Optical Carrier (OC) standards. There are different levels of OC, with OC3 being a common type of Internet connection for large networks as it can carry voice, video, and other data at a transfer rate of 155.52 Mbps.

Internet service providers are now offering fiber to the home so that residential customers can get faster speeds than what are typically offered by DSL and cable connections. Fiber-to-the-home connections can have transfer rates of 150 Mbps!

## *Satellite*

Satellite Internet services come in two basic flavors: one-way with terrestrial return and two-way. Because satellites providing service in most residential areas were designed to send data, the first Internet access over satellites involved downloading from the satellite, but data had to be uploaded via dial-up modem. This transmission tied up phone lines, and upload speeds were rather slow. Two-way systems added technology to return a signal to the satellite. Speeds for uploads ran in the neighborhood of only 1 Mbps, but they did free up phone lines. Download speeds over satellite systems rival those of broadband services (such as ADSL and cable). Just like satellite television, satellite Internet is susceptible to the weather and elements.

## *Wireless*

Wireless access to the Internet is provided through standard 802.11 (WiFi) wireless networks, which are set up to provide coverage in prescribed areas. In some locations, wireless access is provided for free to customers of certain businesses, or by a municipal government like Fredericton, New Brunswick ([www.fred-ezone.ca](http://www.fred-ezone.ca)).

Sometimes, a company may set up access points in a wide range of locations, offering access through them as part of a subscription service. These wireless access points allow connectivity but only to the company's website to set up an account. After you set up and pay for an account, you can use any of the company's access points to access the Internet.

For more information about 802.11 networks, read Book 8, [Chapter 2](#).

## ***Line-of-sight wireless Internet service***

A line-of-sight wireless connection is typically used by a company that wants to connect two locations that are spread over a distance to a network. To connect these two locations, the company will typically place large wireless antennas on top of the buildings to allow the antennas to have a clear line of sight between one another with nothing in between to obstruct the wireless signal.

## ***Cellular and mobile hotspot***

A cellular network is the ISP's network you connect your mobile phone to in order to get access to the Internet. Sometimes called *wireless*, 3G, 4G, or 5G, this system makes use of a cellular provider's wireless network (as opposed to 802.11 networking). To connect to a cellular network, you need a cellular modem for your computer or a cellular router for your network. Mobile devices such as smartphones have a cellular adapter built in, but you can also add one to desktop computers and laptops typically with USB. The benefit of this technology is that you can access the Internet from anywhere your wireless provider has coverage. This is the same technology I cover in Book 8, [Chapter 2](#) when discussing WAN cellular.

Speeds will vary with each wireless carrier, but you will see rated speeds anywhere from 384 Kbps up to 4.9 Mbps. Speeds are dependent upon the provider providing service on EDGE (Enhanced Data for GSM Evolution), High Data Rate (HDR), EV-DO (Evolution-Data Optimized, or Evolution-Data Only), or 3G (Third Generation) networks. 4G networks began emerging in 2010, while 5G became common in 2018, driving data speeds to new levels.

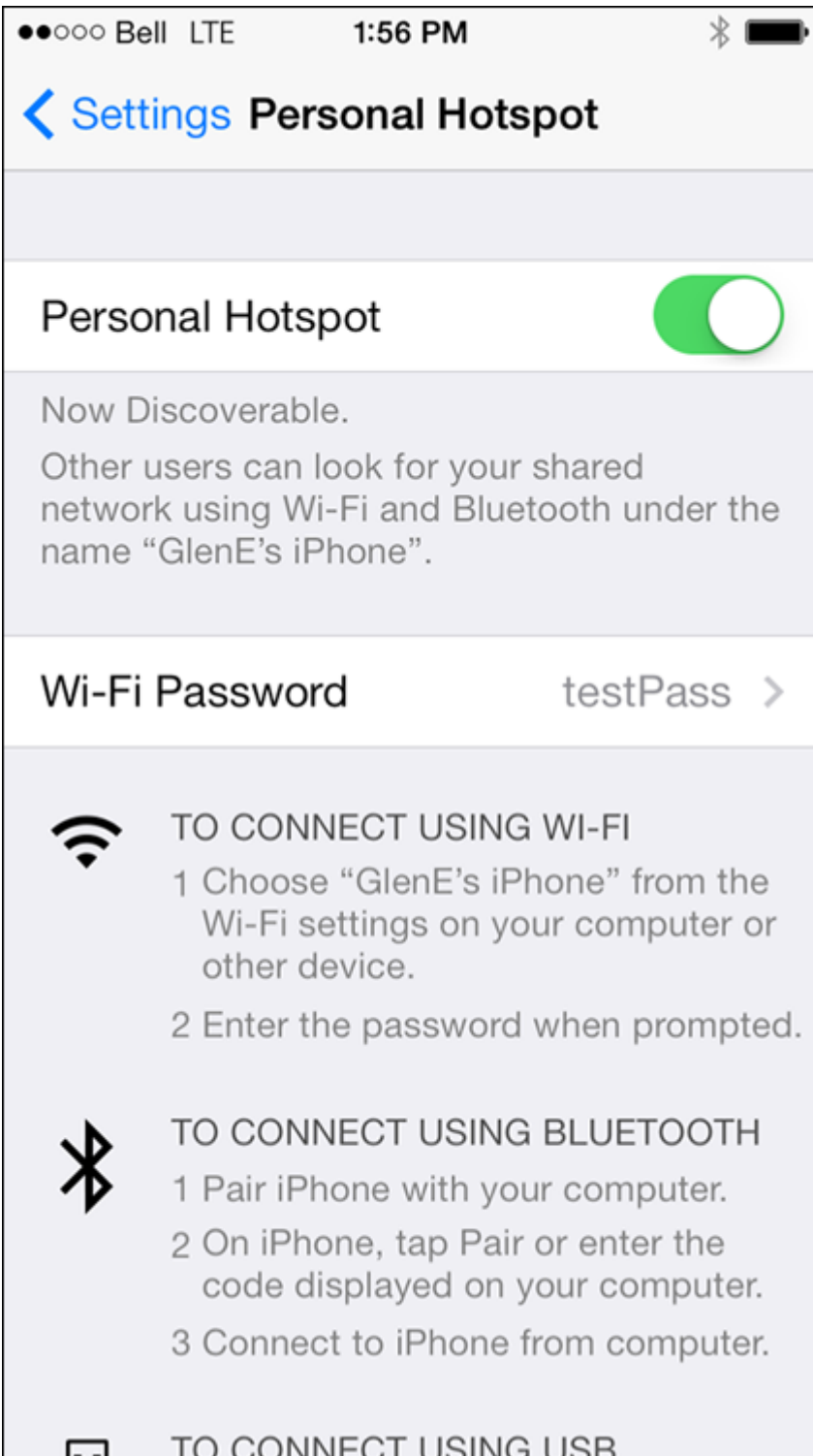
If your mobile device does not have a data plan (meaning you can only use it for phone calls and not surfing the Internet), you can connect your mobile phone or tablet to a mobile hotspot. A mobile hotspot is connected to the service provider's network (3G, 4G, or 5G) and allows other systems to connect to it via wireless in order to gain Internet access. This is similar in concept to your wireless router at home that can give Internet access to your friends and family.

## ***Tethering***

A common method of gaining Internet access on your computer or laptop is by using the Internet connection of your mobile phone. *Tethering* refers to using the Internet connection of your mobile phone by either physically connecting your phone to a laptop (or desktop) via a USB cable or via WiFi or Bluetooth. Once you connect the system to the phone, you are then able to use that phone's Internet connection to browse the Internet.

Many mobile devices give you the capability to easily share your phone's Internet connection. For example, to share the Internet connection off my iPhone, I can make the phone a WiFi hotspot so that a computer can connect to it like any other WiFi network. The steps to share your Internet connection on an iPhone are:

- 1. Log on to your iPhone and choose Settings.**
- 2. Choose Personal Hotspot.**
- 3. Enable Personal Hotspot and then set the password for the hotspot (shown in [Figure 4-12](#)).**



**FIGURE 4-12:** Configuring a wireless hotspot on an iPhone.

Now that your mobile device has been enabled as a personal hotspot, you can connect to it from a wireless client and use the Internet connection of

the phone to surf the Internet.

## ***WiMax***

WiMax is a wireless standard that stands for Worldwide Interoperability for Microwave Access. WiMax is a technology that is designed to cover wide areas like a cellular network, but provide the transfer rate of a wireless network!

# ***Installing a Small Office/Home Office (SOHO) Network***

When installing a *Small Office/Home Office* (SOHO) network — a home office network or a network to be used by a small office with a few employees — you need a number of network components to get the network up and running. This section introduces you to the network components needed to build a small network.

The first major component you need is a home router, which is a multifunctional device that provides you with all the network components needed for your SOHO. The home router acts as a switch that connects all your wired clients together. It also acts as a router that allows you to send data off the network.

You need to decide whether to go wired or wireless, or maybe both. If you opt for wired, you need the appropriate type of cabling to connect each wired client to the network. This is typically UTP CAT 5e or 6 cabling connecting the client to a port on the switch part of the wireless router. If you go wireless, make sure you get a home router that has wireless functionality. Finally, you might want to think about using a server. After the networking nuts and bolts are in place, you then need to think about security.

## ***Functions and benefits of a home router***

A home router has a WAN port that you use to connect to your high-speed Internet connection. This could connect to your cable modem or your DSL

modem, and will be used to share the Internet connection with any users on the network.

The following is a list of benefits to having the home router in your SOHO network:

- » **DHCP:** The first important feature of the home router is a DHCP server, which is responsible for assigning IP addresses to clients on the network so that they can gain network access.
- » **Internet sharing:** The home router will also share the Internet connection that is plugged into the WAN port to all users on the network. This functionality is provided through Network Address Translation (NAT) capabilities. NAT allows you to have one public IP address assigned to one network card on the router so that all systems gain access to the Internet through the one IP address.
- » **Wireless capabilities:** Most home routers are also wireless routers, which allow computers or devices with a wireless card to access the network. The wireless client sends data to the router, which will then be forwarded to the Internet through the WAN port.
- » **Website filters:** Through the configuration of the home router, you can limit which websites users on your network can view. You can also put schedules in place that control when users can use the Internet. Today, home routers provide a number of filtering capabilities to control the type of content that can be surfed.
- » **Network switch:** A home router typically has a four-port switch built in to allow any wired clients to connect to the network. These clients will receive an IP address from the DHCP server built into the router as well so that they can use the network.
- » **Firewall:** A home router has firewall features built in to prevent persons on the Internet from connecting to the systems on your LAN. By default, the firewall is enabled.

To use a home router, simply connect the WAN port of the wireless router to your high-speed Internet connection and then connect your systems to any of the four LAN ports on the router. These systems will get an IP

address from the DHCP server built into the router and then will be able to surf the Internet.

## ***Running a server on a SOHO***

You might eventually look at installing a server for your SOHO. The server performs many different functions, such as holding files that you want to share with other users on the network. The server could also be used to share a printer to all other users on the network.

This server doesn't have to be a system running the Windows Server OS. It could be a Windows 10 system with sharing enabled that shares a folder or printer for everyone else on the network to access.

For more information on sharing printers and files, check out Book 8, [Chapter 3](#).

## ***Wireless networking for a SOHO***

A simple way to allow systems to connect to your network without needing to run cables throughout the entire office or home is to use wireless networking. If you purchase a wireless router, it will allow computers with a wireless network card to connect to the wireless router and any systems connected to it. The wireless client will also be able to surf the Internet because the wireless router will share the Internet connection with not only the wired computers but the wireless systems as well.

To learn more about wireless networking, check out Book 8, [Chapter 2](#).

## ***SOHO security practices***

When building a SOHO network, you have to create a security network structure to protect your business assets. The three chapters in [Book 9](#) give you the foundation to network security, so be sure to read over those three chapters and incorporate them into your SOHO network.

Following is a summary of popular security best practices when creating a SOHO network and using a wireless router:

» **Wireless security:** There are a number of steps to take to secure your wireless network. For more information on wireless networking, check out Book 8, [Chapter 2](#).

- Change the Service Set Identifier (SSID).
- Disable SSID broadcasting.
- Implement MAC filtering.
- Enable an encryption protocol, such as WPA or WPA2.



TIP

To learn more about wireless security, read Book 8, [Chapter 2](#).

» **Router security:** Regardless of whether your router is wireless, look at disabling DHCP and statically assign an IP address to each system. The benefit is that if someone else connects to your network (especially if you have not secured the wireless), he or she will not get an IP address.

» **Firewall:** Use a firewall to protect the network and to protect the systems. A home router has firewall features built in, but you might also look at installing personal firewall software on each system.

» **Administrator password:** Change the usernames for any administrator accounts on your routers and servers if possible. Be sure to set a strong password on these accounts after they are renamed.

» **Update firmware:** To make sure you are dealing with the most up-to-date features on the router, do a firmware update of the router. You can get any updates to the firmware from the manufacturer's website.

Again, this section is definitely not designed to give you details on how to set up a SOHO network, but rather to expose you to the terminology to be familiar with for the A+ exam and some of the considerations with SOHO networking. You can incorporate all the networking and security features covered in [Book 8](#) and [Book 9](#) in your SOHO network, so be sure to read those chapters carefully!



## *Key configuration settings for SOHO networks*

Throughout the chapters in [Book 8](#) and [Book 9](#), you learn about networking concepts and security practices that should be followed when configuring a network and a SOHO network. The A+ certification exams call out the following points to remember when configuring a SOHO network:

- » **Router/switch functionality:** The home router typically gives you a number of ports to connect wired clients together. Each client can connect to one of the ports on the switch part of the home router. The home router will then assign an IP address to each client and allow each client to access the Internet.
- » **Access point settings:** An access point is a device that gives wireless clients access to the network. It has settings that allow you to configure the IP address of the access point, and wireless configuration settings such as the channel, MAC filtering, and encryption settings. If you purchase a wireless home router, this router also acts as your access point for wireless devices.
- » **IP addressing:** One great thing about home routers for SOHO networks is that they have a DHCP server built in that assigns IP addresses automatically to wired and wireless devices. From a configuration point of view, you can control the range of IP addresses that are assigned by the home router.
- » **NIC configuration:** You may need to configure the network cards on some of the networking devices in order to connect them to your SOHO network. For wired network cards, you can configure the duplex (for example, full duplex) and speed (for example, 1000 Mbps) settings. (Note that most network cards autodetect this information.) For wireless connections, you may need to configure the SSID and encryption settings.
- » **End-user device configuration:** When it comes to end-user device configuration, you may need to configure each device for the wireless settings, such as the SSID and encryption settings. End-user devices also include mobile phones wanting to connect to your network.

Usually within the connection settings of these devices you can configure the wireless networking settings.

- » **IoT device configuration:** Internet of Things (IoT) devices may need configuration settings applied such as the wireless network settings and IP address settings if they are not DHCP clients. IoT devices include home appliance devices such as thermostats, light switches, security cameras, door locks, and voice-enabled/smart speakers or digital assistants. All these devices allow you to configure the network settings so that you can access these devices from your mobile phone across the Internet.
- » **Cable/DSL modem configuration:** With your SOHO network, you typically do not need to configure the cable modem or DSL modem with the exception of connecting it to your home router correctly. The cable/DSL modem connects to the WAN or Internet port on your home router, giving you typically four other ports that act as switch ports for clients to connect.
- » **Firewall settings:** One of the big benefits of home routers is that they have a number of features that protect your internal systems (the systems connected via the switch ports or wireless). There are a number of firewall security features that may exist on your home router, including
  - *DMZ:* Some routers have a DMZ port that you can use to connect a server you want to expose out to the Internet. You may want to do this if you are going to host a web server, email server, or DNS server on your network.
  - *Port forwarding:* This allows you to forward specific traffic from the Internet to one of your internal systems based on the TCP or UDP port. You may want to do this if you are hosting a web server or a gaming server inside your network.
  - *NAT:* Network address translation is a feature that converts your internal IP addresses of your clients on the network to use the public IP address of the WAN/Internet port of your home router. This means all outbound traffic appears to be coming

from the one public IP address — essentially hiding your internal address scheme.

- *UPnP*: Universal Plug and Play is a feature on home routers that allows network devices to discover and connect to one another with zero configuration. Your home router must support UPnP as well as the devices that are to discover one another automatically.
  - *Whitelist/blacklist*: Many home routers enable you to block or allow certain devices to access the network. *Whitelisting* is the concept of creating an allow list, while *blacklisting* is the concept of creating a block list. There are different types of whitelist/blacklist: You can have a allow/block by IP address, protocol, or application depending on the home router.
  - *MAC filtering*: This is a feature that allows you to control which systems can connect to the network. As administrators, you can control what systems connect by the MAC address of the network card. This is very common with wireless networking.
- » **QoS**: Quality of Service allows you to prioritize different types of traffic over one another. This ensures the performance for applications that have heavier network bandwidth needs. On many home routers you can give priority to different systems on the network, or to different protocols. For example, on your home network you may prioritize traffic from your Netflix device.
- » **Wireless settings**: Following are key wireless settings that you can configure on your SOHO network:
- *Encryption*: Configure WPA2 as your wireless encryption protocol. This controls who can connect to the network (only someone knowing the key can connect), and encrypts the communication.
  - *Channels*: You can change the channel on your wireless router to help avoid interference with other wireless networks in your area or from cordless phones.

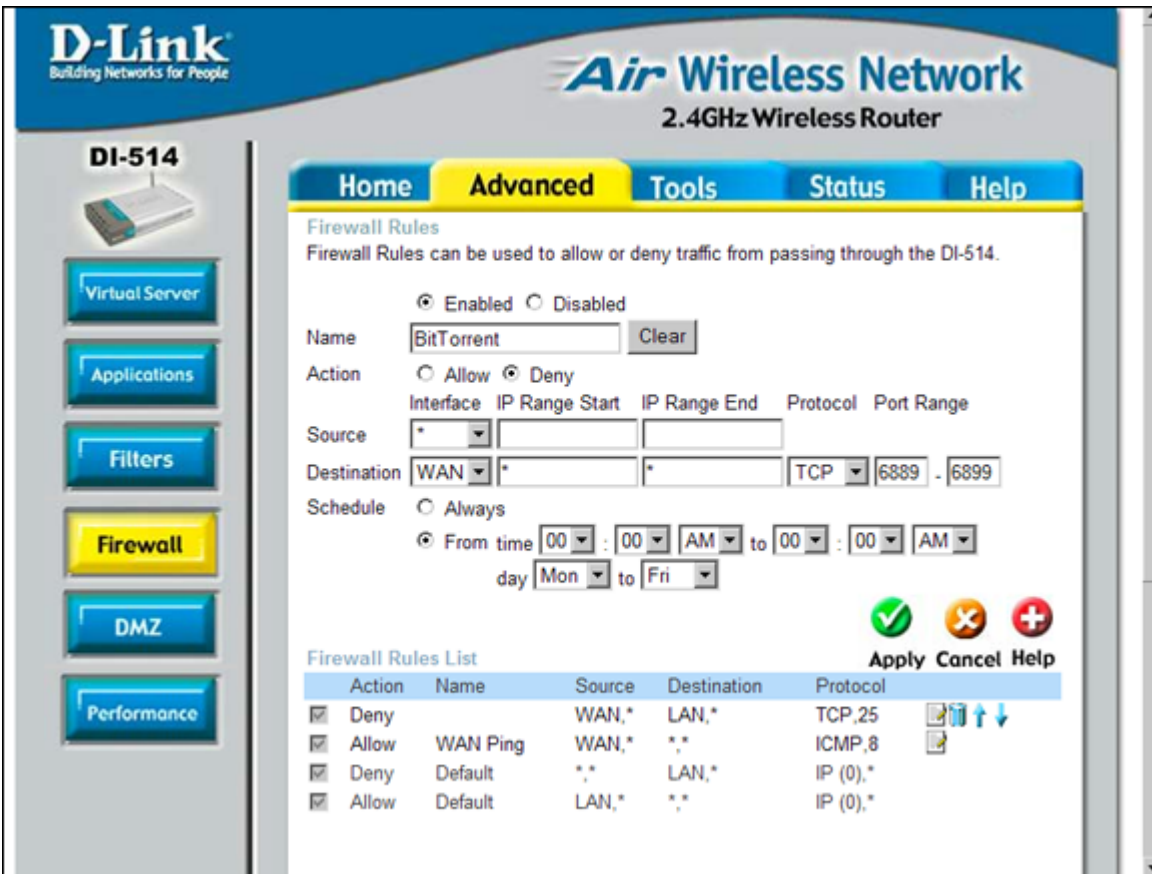
- *QoS*: You can configure quality of service so that different forms of network traffic on your wireless network have higher priority over other traffic.

## *Firewalls and Home Routers*

When dealing with the Internet, remember that a lot of bad things are out there, and you need protection from the dangers of the world. All software firewalls have the inherent problem that they are software running on the system that they are trying to protect, which is considered bad because software (including firewalls) is more susceptible than hardware firewalls to breaches caused by Trojans or other viruses.

Home routers are typically NAT (Network Address Translation) gateways, which allow multiple computers to share one public IP address. This gives you a layer of additional security because only remote servers or computers are allowed to communicate with your computer after you initiate a connection to the remote computer. When you open the connection to the external server, a temporary channel opens to that server's IP address, allowing communication.

Some routers have more advanced firewall features to restrict the TCP and UDP ports that are allowed to be used between the two hosts, as well as the ability to filter or restrict access to URLs based on a series of rules. [Figure 4-13](#) shows some of the security settings available on these devices.



**FIGURE 4-13:** Typical firewall settings on a home router.

In addition to these hardware residential and SOHO (Small Office/Home Office) routers and firewalls, you can choose from various high-end hardware firewalls. Also, Linux firewalls are available that boot directly from CD-ROM, such as Linux Embedded Appliance Firewall (LEAF), IPCop, or SmoothWall. For many Linux firewalls, you need a low-end computer with two network cards and a CD-ROM drive. For a home or small office, even a Pentium or Pentium II processor (or lower if you can find one) will provide enough power for the job.

You find out more about firewalls in Book 9, [Chapter 2](#). The point is that if you are connecting to the Internet, be sure to have a firewall between you and the outside world so that folks on the Internet cannot get in to your system!

## Getting an A+

This chapter provides a brief history of the Internet and how you connect to it. Other concepts that are covered include

- » TCP/IP is the suite of protocols used on Internet.
- » The TCP/IP suite of protocols is made up of other protocols such as FTP, HTTP, `telnet`, `ssh`, TCP, UDP, and IP.
- » POP3, SMTP, and IMAP are the primary protocols used for email.
- » HTML is the formatting system used for Internet web pages.
- » Dial-up, ISDN, T1, ADSL, and cable are the main methods used to connect to the Internet.

## *Prep Test*

### **1. What is the governing body of the Internet?**

- (A) W3.org
- (B) DodNet
- (C) IAB
- (D) IABnet

### **2. The TCP/IP networking protocol is composed of how many subprotocols?**

- (A) 2
- (B) 5
- (C) 10
- (D) Many, too numerous to list

### **3. What purpose does MIME serve?**

- (A) It is used as an encryption method for email.
- (B) It encodes binary data into ASCII data so that it may be sent through email.
- (C) It is used to convert HTML data into an email format.

(D) It is used to trap people inside invisible boxes.

**4. What protocol is used to send email?**

- (A) POP3
- (B) IMAP
- (C) HTTP
- (D) SMTP

**5. What protocols are used to read email? (Choose two.)**

- (A) SMTP
- (B) POP3
- (C) IMAP
- (D) UDP

**6. Which of the following is used to format web pages?**

- (A) HTTP
- (B) WWW
- (C) SSL
- (D) HTML

**7. What protocol is used to transfer files to and from a remote server?**

- (A) HTML
- (B) POP
- (C) FTP
- (D) SMTP

**8. What is the first part of an Internet URL (for example, `http://`) called?**

- (A) Pointer
- (B) Access method

- (C) Control source
  - (D) Activation header
- 9. You are camping during your summer vacation when your manager calls looking for the sales report. There is no wireless network at the campground that you can use to send the report from your laptop. Which of the following identifies the simplest solution?**
- (A) You could use Bluetooth to connect to another camper's wireless network.
  - (B) Copy the file to USB and locate an Internet cafe in the closest town.
  - (C) Turn on airplane mode on your phone and then connect to the wireless hotspot on the phone.
  - (D) You can tether to the Internet connection on your phone.
- 10. You are working as a computer technician at a company. One of the sales people is having trouble connecting to the Internet. You suspect that the proxy configuration setting in the browser is the problem. Which tab in Internet Explorer do you select to allow you to fix the problem?**
- (A) Security
  - (B) Connections
  - (C) Privacy
  - (D) General

## *Answers*

1. **C.** The Internet Architecture Board (IAB) is the managing body of the Internet. See "[\*Understanding the Internet.\*](#)"
2. **D.** Some subprotocols that make up TCP/IP include SMTP, POP3, SNMP, FTP, TFTP, and 500 to 1,000 other protocols. Take a look at "[\*Understanding Internet Protocols.\*](#)"



3. **B.** MIME (Multipurpose Internet Mail Extensions) is used to convert binary files into something that can traverse the text-only email system. *Peek at “[Email](#).”*
4. **D.** SMTP is used to send mail messages over the Internet. *Look over “[SMTP](#).”*
5. **B, C.** POP3 and IMAP are used to read mail that is on a mail server. *Study “[Email](#).”*
6. **D.** HTML (Hypertext Markup Language) is the formatting language or standard for web pages. *Refer to “[Hypertext Markup Language](#).”*
7. **C.** FTP stands for File Transfer Protocol, which is the traditional method to transfer files to or from a server. *Examine “[File Transfer Protocol](#).”*
8. **B.** The first part of a URL represents the access method that is being used to connect to the server. *See “[Using the Internet](#).”*
9. **D.** You could use (tether) the Internet connection on your phone by either connecting the phone to the laptop with a USB cable, or make the phone a wireless hotspot. Note that in order to use WiFi you need to ensure that airplane mode is off. *See “[Tethering](#).”*
10. **B.** The Connections tab in Internet Options has a LAN settings button that allows you to specify the address of the proxy server IE should be using. *See “[Configuring Connections settings](#).”*

# Book 9

# Securing Systems

## Contents at a Glance

### Chapter 1: Fundamentals of Security

[Identifying Types of Attacks](#)

[Understanding Physical Security](#)

[Understanding Authentication and Authorization](#)

[Methods of Securing Transmissions](#)

[Do Not Forget about Data Protection](#)

[Prevention Methods and Best Practices](#)

[Troubleshooting Mobile OS and Device Security](#)

[Introduction to Incident Response](#)

[Getting an A+](#)

[Prep Test](#)

[Answers](#)

### Chapter 2: Implementing Security

[Securing Systems through BIOS/UEFI](#)

[Understanding Logical Security Concepts](#)

[Implementing Users and Groups](#)

[Implementing Permissions and Rights](#)

[Implementing Auditing](#)

[Implementing Firewalls](#)

[Implementing Security Best Practices](#)

[Getting an A+](#)

[Prep Test](#)

[Answers](#)

### Chapter 3: Viruses and Malicious Software

[My Computer Has a Virus!](#)

[Understanding Malicious Software](#)

[Identifying Hoaxes](#)

[Preventing Problems by Staying Up to Date](#)

[Recovering an Infected System](#)

[Getting an A+](#)

[Prep Test](#)

[Answers](#)

# Chapter 1

## Fundamentals of Security

---

### IN THIS CHAPTER

- » Understanding types of attacks and physical security
  - » Understanding authentication and authorization
  - » Looking at the types of data protection
  - » Learning prevention methods and best practices
- 

One of the most important skills to have if you are going to support networked systems or systems connected to the Internet is the capability of securing systems and networks. And even if you are not working in a networked environment, you can apply these same skills to your customers with home Internet machines. The bottom line is that you need a solid understanding of network security.

I remember when a close friend of mine had his website totally replaced by a hacker. My friend's website files were replaced with inappropriate content, and he wondered how on Earth someone had hacked his server. It seems amazing now, but back then (circa 1994), a lot of companies did not use firewalls because they were not aware of the risks involved in having a computer connected directly to the Internet. Back then, people thought, "I have a password on the administrator account, so I am secure."

In this chapter, I introduce you to the basic concepts and terminology used to help secure an environment. Be sure to read this chapter carefully and make sure you understand the topics as you will be tested on security topics on the A+ exams. Have fun with this topic area — it is very exciting!

## *Identifying Types of Attacks*

To me, a hacker is someone with the technical expertise to bypass the security of a network or an OS. A hacker knows how to use features of a piece of software or hardware to gain access to restricted areas of a network and then how to use those features against you and your system. For example, most websites connect to a database behind the scenes so that you can get a list of products when you visit their site. A hacker knows how to input data into the site to manipulate your database server into executing the code that the hacker wants to execute — and this happens because the hacker understands the technologies being used.

The three types of hackers are

- » **White-hat hackers**, who try to “hack” or break software or hardware so as to understand how to protect the environment from black-hat hackers. These are the good guys.
- » **Black-hat hackers** break into a system or network for malicious reasons or for personal gain. The reasons could be for financial gain, bragging rights, or revenge.
- » **Gray-hat hackers** are typically security professionals who exploit systems not for malicious intent, but to report weaknesses in a product to the owners.



**REMEMBER** Hackers use a number of different types of attacks to hack into a network or an OS. Sometimes an attack lays the groundwork for a future or different type of attack: That is, the initial attack does not seem all that dangerous, but it is used in the future to gain unauthorized access.

This section outlines some of the most popular types of attacks that can happen in networking environments today.

## ***Social engineering attacks***

A *social engineering attack* occurs when a hacker tries to obtain information or gain access to a system through social contact with a user.

Typically, the hacker poses as someone else and tries to trick a user into divulging personal or corporate information that allows the hacker access to a system or network.

For example, a hacker calls your company's phone number, listed in the phone book, and poses as a technical support person for your company. He tells the user who answers the phone that a new application has been deployed on the network, and for the application to work, the user's password must be reset. After the password is reset to what the hacker wants, he might "verify" with the user the credential that the user uses. A user who is not educated on social engineering might divulge important information without thinking.



**FOR THE  
EXAM**

A social engineering attack is an attack where a hacker tries to trick a user or administrator into divulging sensitive information through social contact. After the sensitive information is obtained, the hacker can then use that information to compromise the system or network.

This example might sound unrealistic, but it happens all the time. If you work for a small company, you might not experience a social engineering attack. In a large corporate environment, though, it is extremely possible that a social engineering attack would be successful if the company does not educate its users. A large company usually has the IT staff or management located at the head office, but most branch locations have never talked to IT management, so those branch employees would not recognize the voices of the IT folks. A hacker could impersonate someone from the head office, and the user at the branch office would never know the difference.

There are a number of popular social engineering attacks scenarios — and network administrators are just as likely to be social engineering victims as "regular" employees, so they need to be aware. Here are some popular social engineering scenarios:

- » **Hacker impersonates IT administrator.** The hacker calls or emails an employee and pretends to be the network administrator. The hacker tricks the employee into divulging a password or even resetting the password.
- » **Hacker impersonates user.** The hacker calls or emails the network administrator and pretends to be a user who forgot her password, asking the administrator to reset her password for her.
- » **Hacker emails program.** The hacker typically emails all the users on a network, telling them about a security bug in the OS and that they need to run the `update.exe` file attached to the email. In this example, the `update.exe` is the attack — it opens the computer up so that the hacker can access the computer.



**TIP**

Educate your users never to run a program that has been emailed to them. Most software vendors, such as Microsoft, state that they will never email a program to a person: Instead, they will email the URL to an update, but it is up to the person to go to the URL and download it. A great book to learn more on the process a hacker takes to compromise a system is Kevin Beaver's *Hacking For Dummies*, 6th Edition (Wiley).

## ***Phishing***

*Phishing* is a type of social engineering that involves the hacker sending you an email that is impersonating a site such as a bank or an online site like eBay. The email message typically tells you that a pressing matter exists, such as a security compromise with your account, and that you need to log on to your account to verify your transactions. The email message gives you a link to use to navigate to the site, but instead of navigating to the real site, the hacker is leading you to a fake site that he or she has created. This fake site looks like the real site, but when you type in your username and password, the hacker captures that information and then uses it to access your account on the real site!

One form of phishing is known as spear phishing. *Spear phishing* is a phishing attack that is targeted toward a specific individual or company. While phishing is a general email sent out to anyone, spear phishing is targeting a specific person or company in hopes of tricking that person into compromising security.

It is important to educate employees about phishing attacks and know that they should not click the link that is available in the email message. Navigate to the site manually through the browser by typing the URL yourself.

### ***Shoulder surfing***

*Shoulder surfing* is another type of social engineering attack where someone hangs out behind you and watches what you type on the keyboard. The person is hoping to discover sensitive information such as a password. The key to protect against shoulder surfing is to educate employees and inform them that they should never type sensitive information while someone is looking over their shoulder or at their screen.

### ***Network-based attacks***

A *network-based attack* uses networking technologies or protocols to perform the attack. Here are the most popular types.



FOR THE  
EXAM

Ensure that you are familiar with the different types of network-based attacks for the A+ exams.

### ***Password attacks***

There are a number of different types of password attacks. For example, a hacker could perform a *dictionary attack* against the most popular user accounts found on networks. With a dictionary attack, hackers use a program that typically uses two text files:

- » One text file contains the most popular user accounts found on networks, such as administrator, admin, and root.



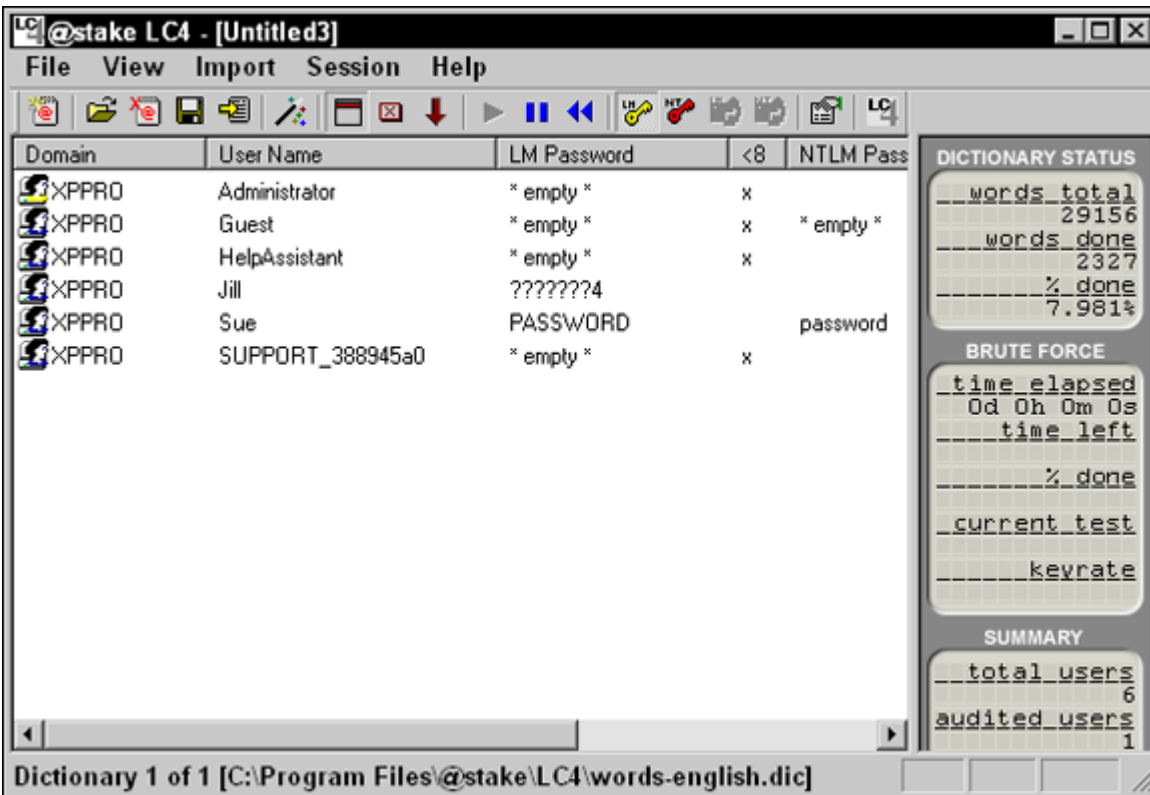
- » The second text file contains a list of all the words in the English dictionary, and then some. You can also get dictionary files for different languages.

The program then tries every user account in the user account file with every word in the dictionary file, attempting to determine the password for the user account.

To protect against a dictionary attack, be sure employees use strong passwords that mix letters and numbers. This way, their passwords are not found in the dictionary. Also, passwords are normally case sensitive, so educate users on the importance of using both lowercase and uppercase characters. That way, a hacker not only has to guess the password but also the combination of uppercase and lowercase characters.

Also remind users that words found in *any* dictionary are unsafe for passwords. This means avoiding not only English words, but also French, German, Hebrew ... even Klingon!

Hackers can also perform a *brute force attack*. With a brute force attack, instead of trying to use words from a dictionary, the hacker uses a program that tries to figure out your password by trying different combinations of characters. [Figure 1-1](#) shows a popular password-cracking tool known as LC4. Tools like this are great for network administrators to audit how strong their users' passwords are.



**FIGURE 1-1:** Cracking passwords with LC4.



**FOR THE  
EXAM**

To protect against password attacks, users should use strong passwords, which is a password comprising of letters, numbers, and symbols with a mix of uppercase and lowercase characters and a minimum length of eight characters.

Another important concept related to password cracking is *rainbow tables*. Let's talk about where they fit in. When a hacker wants to perform a brute force attack, the hacker needs time for the program to calculate all possible passwords based on the criteria given. This could take a very long time! To reduce the time it takes, hackers can use rainbow tables, which are files that already contain all the mathematically calculated passwords. The benefit of rainbow tables is that it gives the hacker the strength of a brute force attack, but the speed of a dictionary attack due to the fact that when the attack is happening, the hacker runs software that just needs to read the precalculated passwords from a file.

## *Denial of service*

Another popular network attack is a *denial of service (DoS)* attack, which can come in many forms and is designed to cause a system to be so busy that it cannot service a real request from a client, essentially overloading the system and shutting it down.

For example, say you have an email server, and a hacker attacks the email server by flooding the server with email messages, causing it to be so busy that it cannot send anymore emails. You have been denied the service that the system was created for.

There are a number of different types of DoS attacks: for example, the ping of death. The hacker continuously pings your system, and your system is so busy sending replies that it cannot do its normal function.



**TIP**

To protect against denial of service attacks you should have a firewall installed and also keep your system patched.

## *DDoS*

A Distributed Denial of Service (DDoS) attack is when multiple systems are used by the hacker to attack a single system. The fact that multiple systems are used to perform the attack means that the attacker can generate more traffic to overload the victim's single system.

## *Spoofing*

*Spoofing* is a type of attack in which a hacker modifies the source address of a network *packet*, which is a piece of information that is sent out on the network. This packet includes the data being sent but also has a header section that contains the source address (where the data is coming from) and the destination address (where the data is headed). If the hacker wants to change “who” the packet looks like it is coming from, the hacker modifies the source address of the packet.

There are three major types of spoofing — MAC spoofing, IP spoofing, and email spoofing. MAC spoofing is when the hacker alters the source MAC address of the packet, IP spoofing is when the hacker alters the

source IP address in a packet, and email spoofing is when the hacker alters the source email address to make the email look like it came from someone other than the hacker.

An example of a spoof attack is the smurf attack, which is a combination of a denial of service and spoofing. Here is how it works:

1. The hacker pings a large number of systems but modifies the source address of the packet so that the ping request looks like it is coming from a different system.
2. All systems that were pinged reply to the modified source address — an unsuspecting victim.
3. The victim's system (most likely a server) receives so many replies to the ping request that it is overwhelmed with traffic, causing it to be unable to answer any other request from the network.



**TIP**

To protect against spoof attacks, you can implement encryption and authentication services on the network.

### ***Eavesdropping attack***

An *eavesdropping attack* occurs when a hacker uses some sort of packet sniffer program to see all the traffic on the network. Hackers use *packet sniffers* to find out login passwords or to monitor activities. [Figure 1-2](#) shows Microsoft Network Monitor, a program that monitors network traffic by displaying the contents of the packets. There are other sniffer programs available such as WireShark and Microsoft's Message Analyzer.

Frame	Time	Src MAC Addr	Dst MAC Addr	Protocol	Description	Src Out
1	0.510735	LOCAL	XEROX 000002	Bone	Security Check (0x03)	
2	8.852730	LOCAL	000C29DF8F0C	TCP	....S., len: 0, seq:3110853661-311085366...	XPPRO
3	8.872759	000C29DF8F0C	LOCAL	TCP	.A..S., len: 0, seq:3238993955-323899395...	10.0.0.
4	8.882773	LOCAL	000C29DF8F0C	TCP	.A...., len: 0, seq:3110853662-311085366...	XPPRO
5	8.912816	000C29DF8F0C	LOCAL	FTP	Resp. to Port 1630, '220 Microsoft FTP Serv...	10.0.0.
6	9.022975	LOCAL	000C29DF8F0C	TCP	.A...., len: 0, seq:3110853662-311085366...	XPPRO
7	10.535149	LOCAL	XEROX 000002	Bone	Security Check (0x03)	
8	12.347756	LOCAL	000C29DF8F0C	FTP	Req. from Port 1630, 'USER administrator'	XPPRO
9	12.357770	000C29DF8F0C	LOCAL	FTP	Resp. to Port 1630, '331 Password required ...	10.0.0.
10	12.538029	LOCAL	000C29DF8F0C	TCP	.A...., len: 0, seq:3110853682-311085368...	XPPRO
11	15.432191	LOCAL	000C29DF8F0C	FTP	Req. from Port 1630, 'PASS P@ssw0rd'	XPPRO
12	15.452220	000C29DF8F0C	LOCAL	FTP	Resp. to Port 1630, '230 User administrator...	10.0.0.
13	15.642493	LOCAL	000C29DF8F0C	TCP	.A...., len: 0, seq:3110853697-311085369...	XPPRO
14	16.884279	LOCAL	000C29DF8F0C	FTP	Req. from Port 1630, 'PORT 10,0,0,2,6,96'	XPPRO
15	16.894293	000C29DF8F0C	LOCAL	FTP	Resp. to Port 1630, '200 PORT command succe...	10.0.0.
16	16.894293	LOCAL	000C29DF8F0C	FTP	Req. from Port 1630, 'NLST'	XPPRO
17	16.904308	000C29DF8F0C	LOCAL	FTP	Resp. to Port 1630, '150 Opening ASCII mode...	10.0.0.
18	16.904308	000C29DF8F0C	LOCAL	TCP	....S., len: 0, seq:3741928937-374192893...	10.0.0.
19	16.904308	LOCAL	000C29DF8F0C	TCP	.A..S., len: 0, seq:3112918220-311291822...	XPPRO
20	16.914322	000C29DF8F0C	LOCAL	TCP	.A...., len: 0, seq:3741928938-374192893...	10.0.0.
21	16.914322	000C29DF8F0C	LOCAL	FTP	Data Transfer To Client, Port = 1632, size 13	10.0.0.
22	16.914322	000C29DF8F0C	LOCAL	TCP	.A...F, len: 0, seq:3741928951-374192895...	10.0.0.
23	16.914322	LOCAL	000C29DF8F0C	TCP	.A...., len: 0, seq:3112918221-311291822...	XPPRO
24	16.944365	LOCAL	000C29DF8F0C	TCP	.A...F, len: 0, seq:3112918221-311291822...	XPPRO
25	16.954380	000C29DF8F0C	LOCAL	TCP	.A...., len: 0, seq:3741928952-374192895...	10.0.0.
26	17.054524	LOCAL	000C29DF8F0C	TCP	.A...., len: 0, seq:3110853723-311085372...	XPPRO
27	17.054524	000C29DF8F0C	LOCAL	FTP	Resp. to Port 1630, '226 Transfer complete.'	10.0.0.
28	17.254812	LOCAL	000C29DF8F0C	TCP	.A...., len: 0, seq:3110853723-311085372...	XPPRO
29	20.559564	LOCAL	XEROX 000002	Bone	Security Check (0x03)	

**FIGURE 1-2:** Using Network Monitor to analyze FTP logon traffic.

Notice in [Figure 1-2](#) that the highlighted packet (frame 8) shows someone logging on with a username of `administrator`; in frame 11, you can see that this user has typed the password `P@ssw0rd`. In this example, the hacker now has the username and password of a network account by eavesdropping on the conversation!



**TIP** To protect against eavesdrop attacks you should encrypt network traffic.

### *Man-in-the-middle*

A *man-in-the-middle attack* involves the hacker monitoring network traffic but also intercepting the data, potentially modifying the data, and then sending out the modified result. The person the packet is destined for never knows that the data was intercepted and altered in transit.



**TIP**

To protect against man-in-the-middle attacks you should restrict access to the network and implement encryption and authentication services on the network.

### *Session hijacking*

A *session hijack* is similar to a man-in-the-middle attack, but instead of the hacker intercepting the data, altering it, and sending it to whomever it was destined for, the hacker simply hijacks the conversation — a *session* — and then impersonates one of the parties. The other party has no idea that he is communicating with someone other than the original partner.



**TIP**

To protect against session hijacking attacks, you should restrict access to the network and implement encryption and authentication services on the network.

### *Wireless attacks*

There are a number of different attacks against wireless networks that you should be familiar with. Hackers can crack your wireless encryption if you are using a weak encryption protocol such as WEP. Hackers can also spoof the MAC address of their system and try to bypass your MAC address filters. Also, there are wireless scanners such as Kismet that can be used to discover wireless networks even though SSID broadcasting is disabled.



**TIP**

To protect against wireless attacks, you should implement encryption protocols such as WPA2 and use an authentication server such as a RADIUS server for network access. For more information on wireless, check out Book 8, [Chapter 2](#).

### *Zero-day attack*

A *zero-day attack* is an attack against a system that exploits a security vulnerability that is unknown to the vendor of the system or software. Zero-day attacks are hard to protect against because the weakness in the product is not yet known, and the vendor does not have any patches or fixes for it.

### ***Zombie/botnet attack***

A system that a hacker has compromised and has full control of is known as a *zombie system*. A hacker will typically use a zombie system, or multiple zombie systems (known as a *botnet*), to attack another system in a distributed denial of service (DDoS) attack.

### ***Software-based attacks***

Just as there are a number of different types of network attacks, there are a number of software attacks as well. As you can likely guess, a *software attack* comes through software that a user runs. The most popular software attacks are mentioned in the sections that follow, and you should be familiar with them for the A+ exams.

### ***SQL injection***

An *SQL injection attack* occurs when the hacker sends `Transact SQL` statements (statements that manipulate a database) into an application so that the application will send those statements to the database to be executed. If the application developer does not validate data inputted in the application, the hacker can modify the data or even delete it. The hacker can potentially manipulate the OS through the application that sends the input to the database.

### ***Buffer overflow***

A very popular type of attack today is a *buffer overflow attack*, which involves the hacker sending more data to a piece of software than it is expecting. The information sent to an application is typically stored in an area of memory (a *buffer*). When more data than expected is sent to the application, the information is stored in memory beyond the allocated buffer. If the hacker can go beyond the allocated buffer, he can run the code. This code executes in the context of the user account associated with the software that was hacked — normally an administrative account!



TIP

To protect against buffer overflow attacks, you should keep the system and its applications patched.

## *Malicious software (malware)*

Malicious software, also known as malware, is any software that does harm to the system, such as a virus or spyware. In the following sections, you get an overview of the different types of malicious software, but be sure to review Book 9, [Chapter 3](#) for more information on malware!

### *Virus*

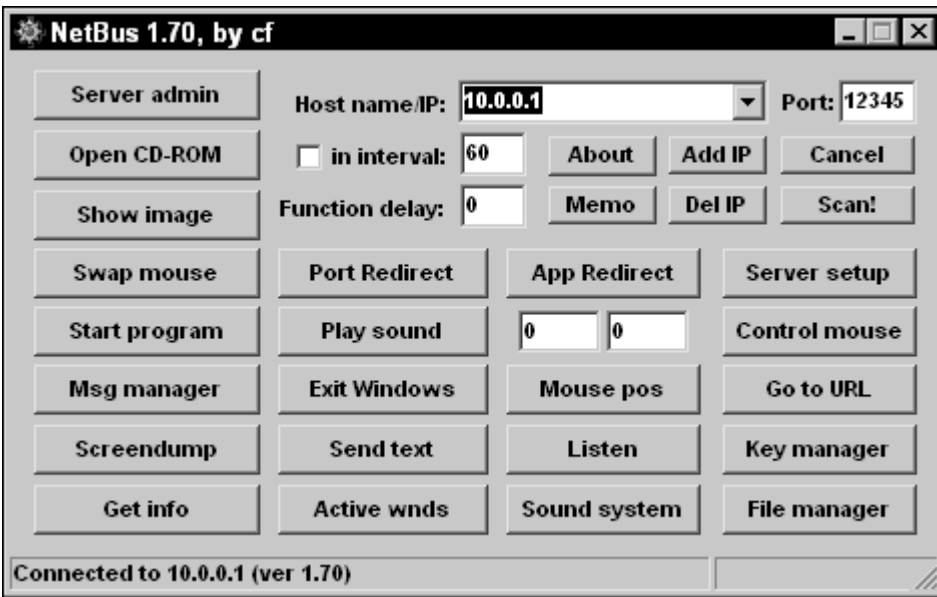
A *virus* is a program that causes harm to your system. Typically, viruses are spread through emails and are included in attachments, such as word processing documents and spreadsheets. The virus can do any of a number of things: delete files from your system, modify the system configuration, or email all your contacts in your email software. To prevent viruses, install antivirus software and do not open any file attachments that arrive in your email inbox that you are not expecting.

### *Trojan virus*

A *Trojan virus* is software that a user is typically tricked into running on the system; when the software runs, it does something totally different than what the user expected it to do. For example, NetBus (an older attack) is an example of a Trojan horse program sent as a file called `patch.exe`. The user receiving the file, typically through an email, believes that the file will fix a security issue. The problem is that `patch.exe` is a Trojan horse, and when that horse starts running, it opens the computer up to allow a hacker to connect to the system.

The hacker then uses a client program, like the one shown in [Figure 1-3](#), to connect to the system and start messing with the computer. The hacker can do things like launch other programs, flip your screen upside-down, eject your CD-ROM tray, watch your activity, and modify or delete files!





**FIGURE 1-3:** Using NetBus to control a user's computer.

### ***Rootkit***

A rootkit is malicious software installed on your system by the hacker that gives the hacker unauthorized access to the system at a later time. You find out more about rootkits in Book 9, [Chapter 3](#).

### ***Worm***

A *worm* is a virus that does not need to be activated by someone opening the file. The worm is *self-replicating*, meaning that it spreads itself from system to system, infecting each computer. To protect against a worm, you should install a firewall. A *firewall* is a piece of software or hardware that prevents someone from entering your system.

### ***Logic bomb***

A *logic bomb* is malicious software that could run every day, but the software was designed to wreak havoc on your system on a certain date and time. The scary thing about logic bombs is that they seem like useful software until the day the programmer decides it will become malicious!

### ***Spyware and adware***

*Spyware* is a type of malicious software that when installed on your system, monitors your activity, including Internet activity. *Adware* is software that after being installed on your system, will pop up with ads

promoting different products and websites. Be sure to install spyware protection and adware protection on your system to prevent such software from running on your computer.

A term sometimes used by security professionals to describe software that performs unwanted actions is *grayware*. Grayware encompasses malicious software such as adware and spyware. Be sure to have malware protection software loaded on your system to protect against forms of grayware.

### ***Ransomware***

*Ransomware* is a type of malicious software that takes control of a system by having a window pop up onscreen letting you know that the system has been locked and that to unlock it, you need to call a number shown on the screen and provide a credit card number.



**TIP** To protect against malicious software such as a virus, Trojan, worm, and a logic bomb, you should use a firewall and keep your virus definitions up to date. To find out more about malicious software, check out Book 9, [Chapter 3](#).

## ***Understanding Physical Security***

You should implement security in many places, and one of the most overlooked areas is physical security. *Physical security* has nothing to do with software; rather, it covers how you protect your environment and systems by making sure that a person cannot physically access the system. For example, many companies use a numeric keypad to secure entrance to a facility. To get into the facility, users must enter a valid combination to open the door.

Another example of physical security is the server room. Most server room doors are locked with a traditional door lock, or a numeric padlock. Higher-security server rooms sometimes use biometric locks that require a fingerprint or retinal scan from anyone trying to enter the room. The

benefit of locking your servers in the server room is hackers cannot boot off a bootable drive such as an optical disc or USB drive, which could allow them to bypass the OS entirely. If someone is able to bypass the OS, he or she typically can bypass the operating system security features of that system. Note that it is common for companies to not only have the server in a locked server room, but also to use server locks where the servers are placed in a locked server rack to prevent unauthorized access to those servers.

A big part of physical security is locking doors to prevent unauthorized access to certain areas of the building, but in high-secure environments, that is not enough because of tailgating! *Tailgating* is when an employee unlocks a door and enters the facility, and an unauthorized person slips through the door with him. To prevent tailgating, the company should use a *mantrap*, which is two locked doors that someone must pass through to gain access to the facility. The hook is that the second door does not open until the first door is locked again. This allows the employee to be aware of who is entering the facility with him before unlocking the second door.



**TIP**

You can apply enterprise security best practices to your home systems. For example, to help secure your home system, you might want to prevent booting from a DVD so that an unauthorized person cannot try to bypass your Windows security.

## ***Dumpster diving***

A common form of attack is called “dumpster diving,” which is where a hacker will sift through your garbage trying to find information that will be helpful in some form of attack at a later time. To protect from dumpster diving, be sure to shred all documents that contain sensitive information.

## ***BIOS/UEFI settings***

You can set a number of settings in your system BIOS to help control the security of the system. Be sure to investigate the BIOS settings on your

system to see what security settings you can enable on the system. Here are some popular BIOS/CMOS settings to aid in physical security:

- » **Drive lock:** Drive lock (a popular feature with laptops) is a hard disk specification used to protect access to the drive. To protect access to the drive, there are two drive lock passwords: a user password and a master password. The user password is used by the user wanting to access the system; the master password is used to reset the user password if the user forgets the password. Do not confuse drive lock passwords that prevent booting from the drive with the general CMOS passwords for the system. If the user password and master password are forgotten or lost, the drive is useless.
- » **Passwords:** You can set a power-on password in CMOS to limit who can use the system. If the power-on password is forgotten, it can typically be erased via a jumper on the motherboard or by taking the battery off the motherboard and putting it back in.
- » **Intrusion detection:** Most systems have intrusion detection features that can be enabled through the BIOS that will notify you if the cover is taken off the system. This is designed to alert you if someone opens the cover and takes internal components.
- » **TPM:** The *Trusted Platform Module* (TPM) is a chip on computer hardware used to store cryptography keys that are typically used to encrypt data. A TPM chip can also be used to authenticate a device because it contains a unique key that identifies the chip, or hardware device. Most computers today have a TPM chip, and a number of software solutions (such as Windows BitLocker) can use the TPM chip to encrypt the contents of the drive.

## *Best practices*

To protect your systems, follow these physical security best practices:

- » **Secure server placement.** Lock your servers in a room for which only a select few individuals have the key. You can also use a lock on the server rack to prevent someone from opening the door on the rack and gaining access to the servers.

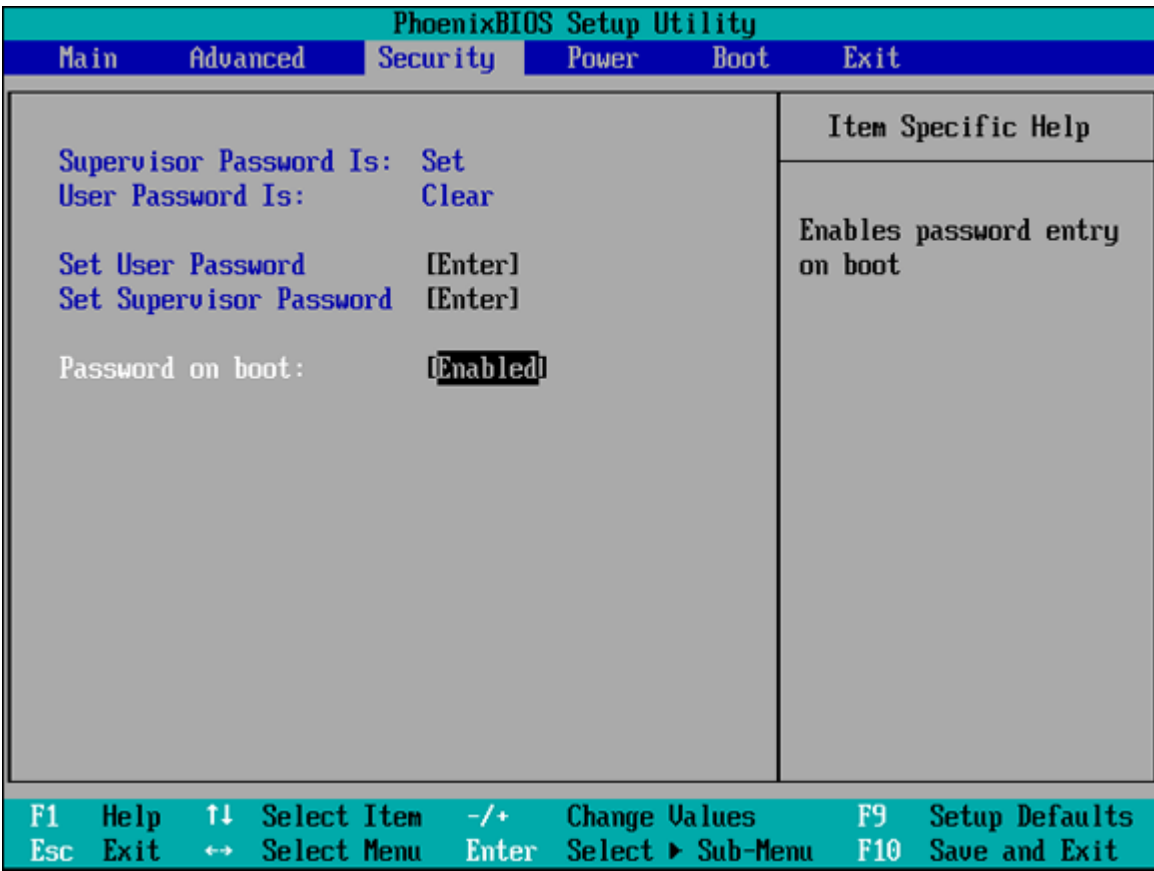
- » **Lock the workstation.** When you leave your system, get in the habit of locking your workstation. A locked workstation can only be unlocked by you or the network administrator. This will prevent other users from accessing the system while you are away.
- » **Disable boot devices.** Disable the ability to boot from a flash drive or DVD-ROM in the CMOS setup on the systems.
- » **Set BIOS/UEFI password.** Because most hackers know how to go into the BIOS and enable booting from DVD-ROM, make sure that you set a password for gaining access to the BIOS/UEFI settings so that a hacker cannot modify your boot devices. [Figure 1-4](#) shows a BIOS password being enabled.



TIP

Check out Book 2, [Chapter 4](#), to get the lowdown on reconfiguring your CMOS settings.

- » **Disable network ports.** To prevent a hacker from entering your office, plugging into the network, and performing a number of network attacks, ensure that network ports, or jacks, in lobbies and front entrances are disabled unless an administrator enables them.
- » **Use a lockdown cable.** Use a *lockdown cable*, also known as a cable lock, to secure laptops, projectors, and other types of office equipment to a table or desk. [Figure 1-5](#) shows a lockdown cable being used to secure a laptop. A lockdown cable usually connects to a special hole in the side of the computer equipment (look for a picture of a lock next to it).



**FIGURE 1-4:** Enabling the BIOS password.



**FIGURE 1-5:** A lockdown cable is used to secure computer equipment to a desk.



FOR THE  
EXAM

Remembering ways to physically secure your systems will help you with the security portion of the A+ exams. Be sure to place critical systems in locked rooms and lock down equipment that is accessible by the public.

## *Understanding Authentication and Authorization*

After you physically secure your environment, focus on the people who access your systems and network. The next step after implementing physical security is to ensure that persons who enter your server room or have a connection to a network port are authorized to log on to the network. Logging onto the network is *authentication*.

### *Authentication*

*Authentication* is the process of proving one's identity to the network environment. Typically, authentication involves typing a username and password on a system before you are granted access, but you could also use biometrics to be authenticated. *Biometrics* is using one's unique physical characteristics, such as a fingerprint or the blood vessels in one's retina, to prove one's identity. [Figure 1-6](#) shows a fingerprint reader used to scan your fingerprint when logging on.



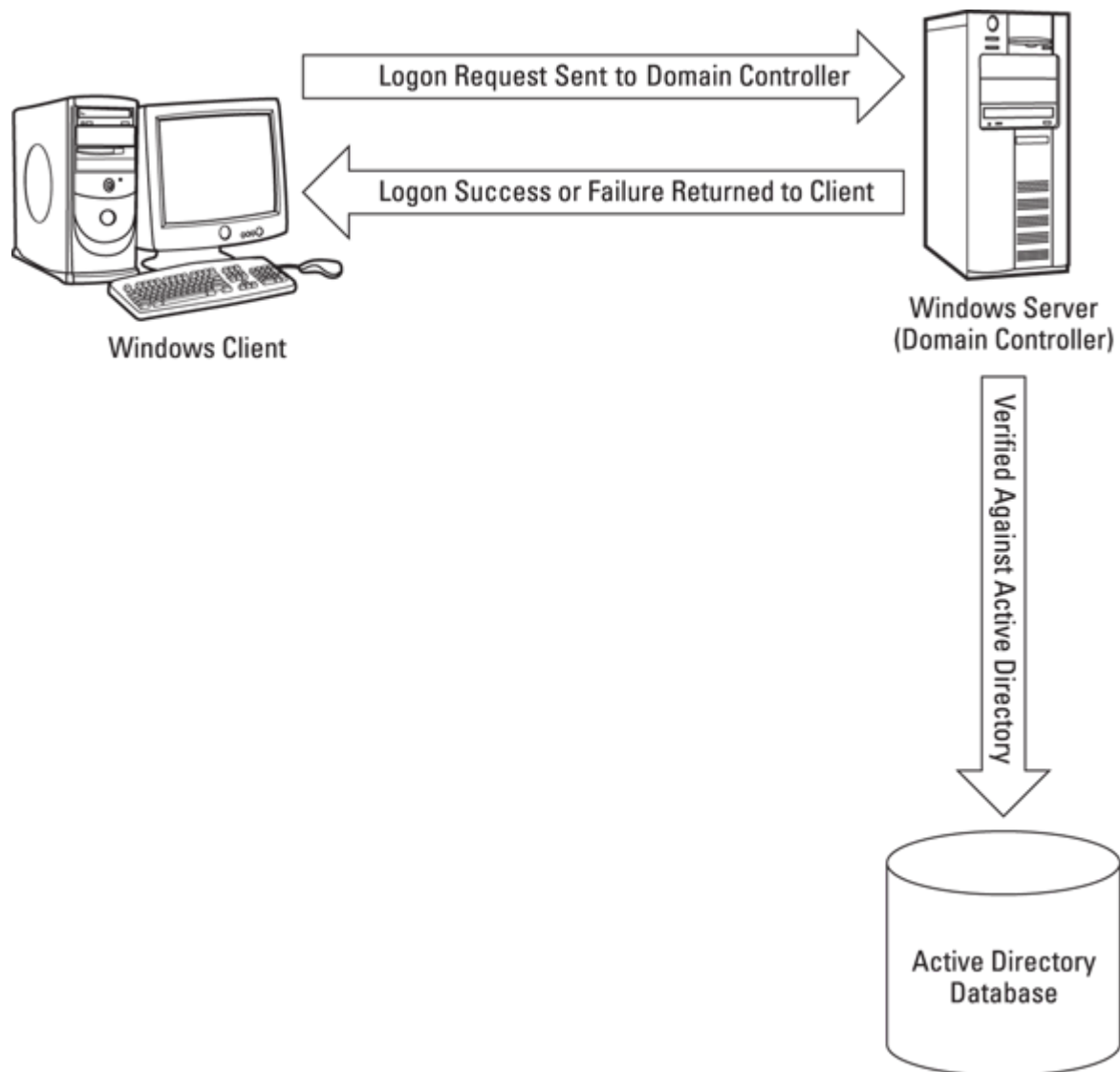


**FIGURE 1-6:** A fingerprint reader is an example of biometrics used for authentication.

Here is a quick look at what happens when you log on to your system with a username and password. When you type a username and password to log on to a system, that username and password are verified against a database — the *user account database* — which has a list of the usernames and passwords allowed to access the system. If the username and password you type are in the user account database, you are allowed to access the system. Otherwise, you get an error message and are not allowed access.

The name of the account database that stores the usernames and passwords is different, depending on the environment. In a Microsoft network, the account database is the *Active Directory Database* and resides on a server known as a *domain controller* (shown in [Figure 1-7](#)).





**FIGURE 1-7:** Logging on to Active Directory in a Microsoft network environment.

### ***Generating the access token***

When you log on to a Microsoft network environment, the username and password you type are placed in a logon request message that is sent to the domain controller to be verified against the Active Directory Database. If the username and password that you typed are correct, an access token is generated for you. An *access token* is a piece of information that identifies you and is associated with everything you do on the computer and network. The access token contains your user account information and any groups of which you are a member. When you try to access a resource on the network, the user account and group membership

in the access token are compared against the permission list of a resource. If the user account in the access token or one of the groups contained in the access token are also contained in the permission list, you are granted access to the resource. If not, you get an access-denied message.

If you do not have a server-based network environment and you are simply running a Windows desktop system such as Windows 8.1, when you log on, the logon request is sent to the local computer — to an account database known as the Security Accounts Manager (SAM) database. When you log on to the SAM database, an access token is generated as well, and that helps the system determine what files you can access.

### ***Smart card***

Another type of logon supported by network environments today is the use of a smart card. A *smart card* is a small, ATM card–like device that contains your account information. You insert the smart card into a smart card reader that is connected to a computer, and then you enter the PIN (personal identification number) associated with the smart card. This is an example of securing an environment by forcing someone to not only have the card but also know the PIN.

### ***Other authentication objects***

When implementing authentication systems, you have a number of different ways that you can prove someone's identity or that he belongs in the physical facility or environment. The most common method to authenticate someone to a system is with a username and password, but the following items outline some other methods of authenticating employees and many of these relate to physical security:

- » **ID badges/Badge reader:** High-secure environments require all personnel, including employees and contractors, to wear identification badges at all times to identify that employee. These badges may also use different colors, which are a flag identifying different parts of the building that the employee is allowed to be in. Some badges have magnetic strips that store authentication information and are used to swipe into a badge reader before gaining access to the building.

- » **Key fobs:** A key fob is a small authentication hardware device that connects to an employee's keychain. The device is used in the authentication process by generating a random number that the employee who possesses the key fob must enter as part of the authentication process. The random number is synchronized with an authentication device. A key fob is also a device that is used to gain access to a building by having the employee swipe the key fob past a scanner.
- » **RFID badge:** RFID (radio frequency ID) badges use radio frequency to submit authentication information to RFID access points as the employee approaches the facility or different areas of the facility. The benefit of the RFID badge is that the employee is not required to swipe any kind of card because the RFID signal is picked up by the access point.
- » **OTP token:** A *One-Time Password* (OTP) token is a device, also called a key fob, that is used in authentication by generating a random number that the user carrying the token, usually on his or her keychain, would use along with his or her password.
- » **USB locks:** USB locks are physical hardware devices that are used to prevent someone from plugging a USB device into your USB ports. In order to remove the USB lock and gain access to the ports, someone would need the key to unlock the USB lock. This helps prevent data theft on a portable USB drive.
- » **Hardware tokens:** A hardware token is a physical security device you are required to have in your possession in order to authenticate to a system. The hardware token can come in many forms, including a key fob or OTP token.
- » **Privacy filters/privacy screens:** Privacy filters, also known as privacy screens, are placed on computer screens so that to see the information on the screen, you have to be directly in front of the screen. The privacy filter is similar in concept to a window blind that sits on top of your computer screen and prevents someone lurking around you from seeing the information on the screen.

- » **Entry control roster:** In high-secure environments you may want to have an entry control roster, which is a list of people allowed to gain access to the facility. The roster usually sits at the entrance to a building or at the gate entrance to the facility. Typically, an employee signs visitors in and records the time they entered and exited the facility.

### *Strong passwords*

It is really hard to talk about authentication without talking about ensuring that users create strong passwords. A *strong password* is a password that is very difficult for hackers to guess or crack because it contains a mix of uppercase and lowercase characters, contains a mix of numbers, letters, and symbols, and is a minimum of eight characters long.

## USING STRONG PASSWORDS

A number of years ago, I had a co-worker who was always trying to get me to guess his passwords. He thought I had some magical trick or program that was cracking them, but all I was doing was guessing his passwords. I remember one time he changed it, and I could not guess it until one night when we were at a social function for work and all he talked about were the Flyers hockey team. I remember sitting there thinking, "I bet that is his password." Sure enough, the next day at work, I tried `flyers` as his password, and it worked! Now the lesson here is that you should use complex passwords. A complex password is a password of at least eight characters, a mix of lowercase and uppercase characters, and uses numbers and symbols. Complex passwords are hard to guess and also more difficult to crack with a password cracker.

### *Single sign-on*

Single sign-on (SSO) is an authentication term you should be familiar with for the A+ exams. SSO is the principle that you should be able to log on to the network with your username and password and then be given access to a number of different resources such as files, printers, and your email using that one username and password. The opposite of an SSO environment is when you have to supply a username and password for each different resource that you access. Microsoft's Active Directory environment is an example of a single sign-on environment.

### *Multifactor authentication*

There are different techniques that can be used to authenticate to an environment:

- » **Something you know:** The most common method of authentication is inputting something you know, such as a PIN or password.
- » **Something you have:** This authentication method involves authenticating by having a physical object in your possession, such as a debit card, a smart card, or a key fob.
- » **Something you are:** This authentication method involves authenticating to a system with personal characteristics of yourself such as a fingerprint scan, retina scan, or voice recognition. This is where biometrics fits in.

The key point here is that in high-secure environments you should use multiple authentication techniques, which is known as multifactor authentication. Let's look at why. If you drop your bank card (something you have) on the ground and someone picks it up, will she gain access to your account? The answer is no; that would be a terrible authentication system if banks granted access based on you having the bank card in your possession. So the bank uses two factors of authentication: You have to have the bank card (something you have) and then you must type the PIN (something you know) associated with the bank card. Requiring both factors greatly increases the security of the scenario. This is known as multi-factor authentication — using more than one of something you know, something you have, and something you are.

It should be noted that most of us log on to a network by typing a username and password, both of which are examples of something we know. For this reason, a username/password authentication technique is not considered multifactor authentication because we are only using one method of authentication.

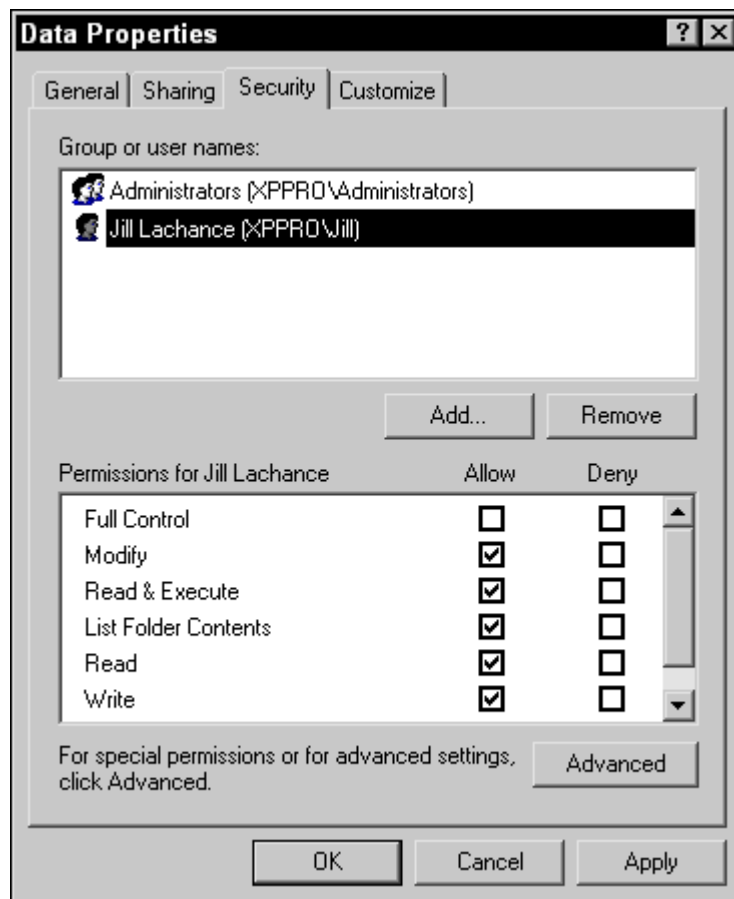
## *Authorization*

After a user logs on and an access token is created, the user may start trying to access resources such as files and printers. To access a file, folder, or printer on the network, the user must be authorized to access the

resource. *Authorization* is the process of giving a user permission to access a resource or the right to perform an OS task. Do not confuse authentication and authorization: You must be first authenticated to the network; then, after authentication, you can access the resources you have been authorized for.

## Permissions

To authorize access to a resource, you set permissions on the resource. For example, if you want to allow Jill to access the accounting folder, you need to give Jill permission to the accounting folder, as shown in [Figure 1-8](#).



**FIGURE 1-8:** Using permissions to authorize which users are allowed to access the resource.

In [Figure 1-8](#), you can see that the Administrators and Jill have access to the resource. No one else is authorized to access the resource. You find

out how to set permissions in the next chapter, but for now, make sure you understand the difference between authentication and authorization.

### ***Rights***

In the Windows world, there is a difference between permissions and rights. As you can read in earlier sections, permission is your level of access to a resource. Comparatively, a right is your privilege to perform an OS task. For example, you can be assigned the right to change the time on the computer. Other examples of rights are the right to do backups or the right to log on to the system.

To learn more about how to set permissions and rights, check out Book 9, [Chapter 2](#).

## ***Methods of Securing Transmissions***

After you authenticate users and authorize them to access certain parts of the network, you should then consider methods of securing information while it travels along the network cable.

Most network communication is sent along the network wire in *cleartext*, meaning that anyone connected to your network can read the information. But if the information is traveling across the Internet, anyone can view that information if it is passed in cleartext.

Most Internet protocols, such as HTTP, send information in cleartext, and it is up to the people who set up the servers that use these Internet protocols to encrypt the information before it is released to the Internet. *Encrypting* the information means that the information is run through a mathematical calculation that generates an altered version of the information: a *result*. For example, the words `Glen Clarke` could be encrypted to look like `7y3i s3fk4r`. If anyone intercepts such encrypted information and views it while it is traveling across the wire, the information would mean nothing.

Here is a real-world example. You type your credit card number on a website, but you certainly do not want that credit card number to be viewed while you send it from your client computer to the server. You

want to be sure that the website where you enter the credit card number encrypts the traffic. You can tell by the lock icon that appears in the web browser, as shown in [Figure 1-9](#).



**FIGURE 1-9:** Identifying a secure site by locating the lock in Internet Explorer.



**FOR THE  
EXAM**

It is important for the A+ exams that you understand popular methods of encrypting traffic. You can use a number of technologies, such as

- » **Secure Sockets Layer (SSL):** This protocol is used to encrypt different types of Internet traffic. For example, you could use SSL to encrypt HTTP traffic by applying a digital certificate to the website. The *digital certificate* contains the key that is used to encrypt and decrypt the traffic.



- » **Internet Protocol Security (IPSec):** This protocol can encrypt all TCP/IP traffic between systems. As a network administrator, you configure IPSec on the server and the clients with the same key or digital certificates, which are used to encrypt and decrypt network traffic. Because of the configuration, it is an unlikely solution for a website but is a great way to encrypt traffic on your network.
- » **Virtual Private Network (VPN):** A VPN allows a user to connect across the Internet to a remote network, typically her office network, and send information between her system and the office network securely. The information is secured because the VPN technology used creates an encrypted tunnel between the user and the office network — any data that travels through the tunnel is encrypted.

The preceding sections touch on a number of places that require security. Here is a quick overview of the security steps that I have discussed so far:

- » Secure your office environment first from physical access by unauthorized persons.
- » Set up a system for authentication, which is the idea that users must log on to the network.
- » After users log on to the network, they must be authorized to access resources.
- » When you allow someone to access resources, make sure that you encrypt the traffic while it is in transit, especially if the information is transmitted outside your own network.

## ***Do Not Forget about Data Protection***

In this section, you find out about how to secure your data environment from a hacker or malicious user. When securing your systems, you want to protect the systems from a person who damages information or systems

with or without intent. You want to be sure to secure your environment from hackers, but at the same time, you want to protect your systems from users on the network who may cause damage without meaning to.

Accidents can happen, so be sure to prevent accidents from happening by following the best practices in the following sections.

## ***Data destruction and disposal***

Most office environments have strict policies in place to help secure confidential information. Shredding paper documents with personal or confidential information is a huge requirement of physical security. Be sure to secure all sensitive documents in a locked cabinet and have shredders available to destroy paper-based documents. It is important to note that computerized data should be no different. A company needs strict guidelines on how to properly destroy data that resides on computer hard drives, flash drives, and DVDs.

### ***Hard drive destruction***

Many highly secure environments do not want to risk the fact that the program used to erase the contents of the drive did not work as expected, so they opt to have the hard drives removed from any system being decommissioned and then physically destroy the drives through one of the following methods:

- » **Shredder:** Destroying data that resides on a computer hard drive typically involves shredding the computer hard drive with a huge shredding machine, or destroying the drive another way, such as sanding the platters down to nothing.
- » **Drill/hammer:** I have talked to some customers who used to destroy drives by drilling spikes through them, but what they found was that the data around the hole that the spike put in the drive could still be read! These customers now disintegrate the drive in a huge shredder. Other customers sand the drives down to nothing. Either way, if securing the data is a concern, make sure to *physically destroy* the entire drive that contains the data.
- » **Electromagnet (Degaussing):** Because the data is stored magnetically on the disk, you could destroy the data from the drive by

using a very strong magnet to magnetically corrupt the data on the drive into an unreadable format. You can use a degaussing tool to magnetically randomize the data stored on the drive to prevent the data from being readable.

- » **Incineration:** Another option to physically destroy hard drives or optical drives (such as DVDs) is to burn the physical media until there is nothing but smoke left!
- » **Certificate of destruction:** A certificate of destruction is a document that validates that indeed the storage media was destroyed. This document is given to the data owners by the storage vendor or person to essentially sign-off on the fact that the media containing sensitive data was destroyed.

### *Hard drive recycling*

Often when replacing a perfectly working hard disk on your system with either a faster disk or one of a larger capacity, you may want to recycle the existing drive by using it in another system, handing it over to another department, or selling/donating it to someone. Before recycling the drive, you want to ensure that any sensitive data on the drive is erased.

### *LOW-LEVEL FORMAT VERSUS STANDARD FORMAT*

When looking to replace a system, recycle it, or donate it to charity, it is critical that you erase all the company data from the drive. Most people look to formatting the drive as a method of erasing the data from the drive, but depending on the type of format you do, the data may actually not be erased. The following are different types of formats that can be performed:

- » **Low-level format (LLF):** A low-level format is performed on the drive at the manufacturer and is responsible for setting up the tracks and sectors on the disk. Low-level formats are normally not done by the administrator or user. You need the LLF program to perform such an operation, which is typically only available to the manufacturer of the drive.

- » **High-level format (HLF):** The high-level format is responsible for setting up the file system on the drive and creating allocation tables such as the file allocation table (FAT) and the directory entry table.
- » **Quick format:** A quick format is the term for the format operation you can perform to “erase” the contents from the drive. It is called a quick format because it doesn't actually erase the data; it simply deletes the entries from the directory entry table (which is a listing of files that exist).

### ***HARD DRIVE SANITATION/DRIVE WIPE/OVERWRITE***

When it comes to erasing the data from the drive, also known as *sanitizing* the drive, it is not enough to perform a format of the drive because formatting the drive does not actually erase the data from the sectors, and someone determined to discover your information can use a forensics tool to view deleted data on the drive. You must use a drive-wiping program, also known as a shredding application, which actually overwrites the contents on the sectors of the drives many times to ensure that the company data no longer exists.

I use a program called *Secure Wipe*, from the Forensics Acquisition Utilities (FAU), to overwrite and sanitize a drive, which you can download from <http://gmgsystemsinc.com/fau>. After you download FAU, you can run the secure wipe program by navigating to a command prompt (to the FAU directory) and then type the following command to securely erase a drive (I am erasing the F: drive in this example):

```
wipe \\.\f:
```

You will notice that the program *overwrites* the contents of the drive three times, the first time writing all FFs to the drive, the second time writing random bits, and the third time writing null values (nothing).



**WARNING** Be aware of the risk of selling or giving your hard drive to someone! Companies concerned with corporate security and data privacy will likely opt to destroy the drive instead of recycling because of the risk of having private data lifted off the drive.

### ***Destroying paper documents***

Not only should you be concerned with the company data that is stored on hard drives electronically, but you should also watch for security issues surrounding confidential data in hard copy format. A business must have paper shredders that are used by employees to shred documents before recycling or placing in the garbage.

Also watch for situations where employees are writing passwords on paper and leaving the paper in an unsecure location. Be sure to educate employees on the importance of not writing passwords on paper.

Make sure that you secure physical documents by having all confidential documents in hard-copy format locked in filing cabinets. Ensure that the filing cabinets are in secure areas where you can control who has physical access to those cabinets.

### ***Backing up data***

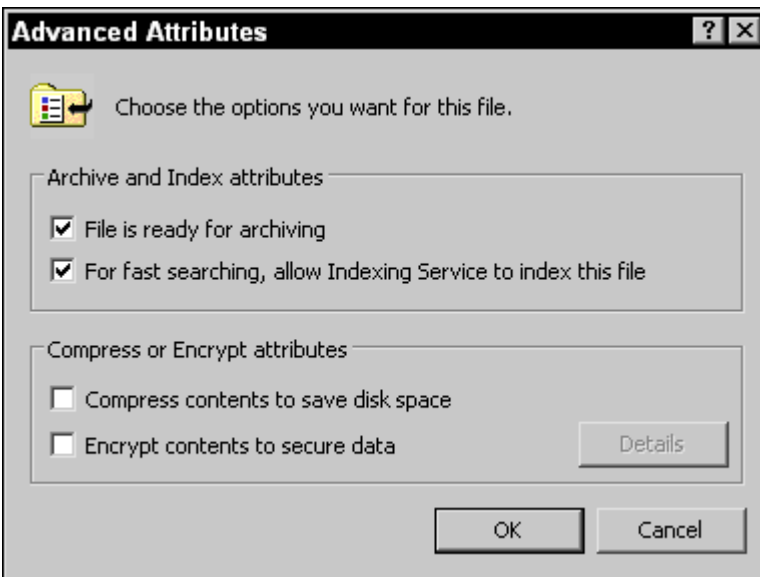
A big part of securing the data environment is not only setting the permissions but also ensuring that you create a good backup and restore strategy. Identify which files are critical to the operation of the business and should be backed up. You also want to be familiar with all types of information used by your company. For example, you might depend on email, so make sure that you back up your email server along with any files in shared folders. If your company stores important data in databases, make sure that you back up those databases as well.

### ***Backup review***

You can find out more about backups in Book 7, [Chapter 3](#), but for the A+ exams, here are some of the key points you need to remember.

When you perform a backup, the OS keeps track of which files have been changed since the last backup by setting the *archive bit*. The archive bit is an attribute of the file that tells the system that the file has changed. To view the archive bit within Windows XP or Windows 7, right-click the file and choose Properties. In the Properties dialog box, click the Advanced button.

The first option in the Advanced Attributes dialog box that appears — File Is Ready for Archiving — is the archive bit. (See [Figure 1-10](#).) When this check box is selected, it means that the file needs to be backed up because it has changed.



**FIGURE 1-10:** Viewing the archive bit in Windows.



**REMEMBER** Before you perform a backup, decide what type of backup to perform. Each backup type deals with the archive bit a little differently. Here are the three major types of backup:

- » **Full backup:** Copies any files that you select, whether the archive bit is set or not, and clears the archive bit on any file that is backed up — essentially recording the fact that the file has been backed up.

- » **Differential backup:** Copies any files that have changed, but it does not clear the archive bit; thus, there is no record that the files have been backed up. The benefit is that the next time you do the backup, the files will be backed up again because the archive bit has not been cleared. As far as the OS is concerned, the file has not been backed up since it was changed.
- » **Incremental:** Copies any file that has changed and then clears the archive bit on any files that are backed up. Thus, if a file is copied during an incremental backup, because the backup process clears the archive bit, the file will not be backed up during subsequent incremental backups unless the file changes again.



FOR THE  
EXAM

Be familiar with the difference between a full, incremental, and differential backup. Also know which backup types clear the archive bit.

### ***Tape rotation and offsite storage***

Take the time to rotate tapes so that the same tape is not used all the time. You also want to make sure that you store a backup offsite in case of a disaster such as flood or fire. It is important that you are able to recover the system no matter what happens.

### ***Test restore operations***

As a last point with backup strategy best practices, you want to test restorations frequently to ensure that you can recover information from backup without any problem. You do not want to find out that the backups are bad when management is hanging over your shoulder waiting for the company network to come back online! Be sure to perform regular test restorations.

### ***Implementing RAID solutions***

To help secure your data, not only do you want to have good backups, but you also want to ensure that you are implementing some form of a RAID

solution. RAID (Redundant Array of Inexpensive Disks) is covered in detail in Book 2, [Chapter 5](#), so in this section I review the different types of RAID volumes supported in Windows servers and ensure that you understand that RAID solutions are a way of helping secure data.

RAID is a way of storing duplicated data on multiple disks; if one disk goes down, the data is still available to the users because other disks in the RAID array have a copy of the data. The benefit of using RAID instead of backups is that with the RAID solution, the user never knows that a drive has failed because the other drive is supplying all the data.

**Note:** You still need the backups, though, in case both drives fail, or some disaster happens, like a flood or fire, destroying the system and all of its drives.

A number of different types of RAID solutions are available. The ones provided by the Windows Server OSes are as follows:

- » **RAID Level 0:** Also known as a *striped volume* in Windows, RAID Level 0 writes different parts of the data to different disks at the same time. The benefit of a striped volume is that you get a performance benefit by writing the data at the same time to two different disks, essentially taking less time to read or write to the file. Note that the data is split between both drives, and there is no duplication — which means that this is not really a redundant solution.
- » **RAID Level 1:** Also known as a *mirrored volume* in Windows. A mirrored volume duplicates the data stored on one disk to another disk. If one disk fails, the other disk has a copy of the data.
- » **RAID Level 5:** Also known as a *RAID 5 volume* in Windows. A RAID 5 volume requires a minimum of three drives and writes to all drives in the solution like a striped volume. A RAID 5 volume is different than a striped volume in the sense that it does store redundant data — *parity data* — on one of the disks. The redundant data is used to calculate the missing data when a disk goes missing, ensuring that users can still retrieve the data without noticing a problem.





FOR THE  
EXAM

Be comfortable with the RAID levels when preparing for the A+ exams. Check out Book 2, [Chapter 5](#), to see how to create volumes in Windows.

## *Data encryption*

Encrypting data converts information to an unreadable format so that if folks gain access to the data, they cannot understand it. In the cryptography world, encryption is described as changing plain text to cipher text. As you can likely intuit, decryption converts cipher text to plain text.

There are a number of ways to encrypt data on the hard drive:

- » **EFS:** The Encrypting File System (EFS) is a feature of NTFS and can be enabled through the file properties. After the file is encrypted, it can be read only by authorized persons. To read more about EFS, check out Book 5, [Chapter 4](#).
- » **BitLocker:** Instead of encrypting data at the file level with EFS, you can have Windows encrypt the entire partition or volume, which protects all data on the partition, including the Windows OS, the Registry, and the data. With BitLocker, data is encrypted by using keys stored in a TPM chip or a USB drive, depending upon how BitLocker has been configured.
- » **Third-party software:** You can also use third-party software to encrypt data. For example, you can use a program such as Folder Lock to encrypt all your data.

## *Compliance and classification*

Part of securing your computing environment is understanding how to protect the business from disclosure of information and by ensuring the business is compliant with government and industry regulations that surround computing and data.

### *Compliance*

Data compliance is the concept of protecting the data from information leaks and ensuring recoverability of information by following government regulations and industry regulations. For example, if you are in the health industry, you must be compliant with the Health Insurance Portability and Accountability Act (HIPAA), which requires that health records and patient information be secured and kept private.

Companies are also required to protect customer information as outlined by the Privacy Act. Companies are no longer allowed to share customer information with other businesses, including contact information such as email addresses and phone numbers.

Another example of data compliance is ensuring that your company has taken the correct steps and implemented the correct controls to adhere to the Sarbanes-Oxley Act, which outlines that the company must be able to prove that adequate auditing controls have been put in place in case an incident requires review of internal information, such as company emails.



**WARNING** If you are the security manager for your company, be sure to spend time researching which government regulations and industry regulations your company falls under. With your list of regulations in hand, then you can determine the steps you need to take to be compliant.

## **NON-COMPLIANT SYSTEMS AND VIOLATION OF SECURITY PRACTICES**

On the note of compliance, a company may have policies around compliant systems and non-compliant systems. A *compliant system* is a system that follows a company security policy and all the rules of operating in a secure environment. A *non-compliant system* is a system that does not meet the company's expectations of operating in a secure environment. For example, a company may have a policy that any system accessing the network must be up to date with patches, have a firewall enabled, and have antivirus software installed and up to date. Not meeting these expectations (violation of security practices) results in immediate disconnection from the network.

## *Classification*

Part of securing company information is through data classification, which assigns a level of sensitivity to information, such as Confidential or Top Secret. After the level of sensitivity is assigned to the information, the necessary controls are put in place to protect that classification of information.

Each data classification has specific security measures that need to be implemented to keep it secure. For example, a company might decide that top secret information cannot leave the “top secret” system — say, by disabling the ports on the system that typically would allow connecting a removable drive.



**REMEMBER** Data classification is assigned to the information based on the value of the information to the organization. Each classification level is designed to indicate whether the information is to be kept private or is available for public release. The following are examples of classification levels:

- » Top secret, secret, and unclassified
- » Confidential, official use only, and public
- » Highly confidential, proprietary, internal use, and public

## *Prevention Methods and Best Practices*

A company can take a number of different steps to help improve the security posture of the organization. In the following sections, you review important methods of improving different aspects of security.

### *Physical security*

Physical security is discussed earlier in the chapter, and it is a big part of any company's security strategy. It is important to ensure that you have servers, routers, and other network equipment locked in a server room.

In highly secure environments, ensure that you have fences around the perimeter of the property, with only one entrance that all persons must pass through. In most high-secure environments, security guards are at the entrance, controlling who gains access to the facility. After people are inside the facility, you can control access to different areas of the building with swipe cards or other authentication devices.

When configuring a system for security, be sure to configure BIOS/UEFI passwords to control who can change the BIOS settings on the system. Also, modify the boot order of the system so that someone cannot boot from an optical disc or USB drive. If employees can boot from another operating system, they may be able to bypass the security of the system.

## *Digital security*

You can take a number of different steps to improve digital security. First ensure that you have software installed on the system to protect you against malicious software. All systems should have antivirus and antispyware software installed.

You should also ensure that firewall software is installed on the system to protect the system from unwanted traffic. Hackers can exploit the system by simply sending a few commands to the system, so it is important that you control what can reach your system. All current versions of Windows have built-in firewall software that can be enabled.

Ensure that you configure strong passwords on your user accounts so that no one can guess or crack your passwords. Passwords should meet the following requirements:

- » Minimum of eight characters
- » Mix of uppercase and lowercase characters
- » Contain a number and symbol
- » Is not a word in the dictionary

You should also ensure that you secure the files and printers on a system with permissions. In Windows, these are called the NTFS permissions, which control who can access what files and what level of access employees should get. For example, you can specify that Bob gets access to the employee handbook document, but that he only gets read access, not write (modify) access!

Following are some technologies that can enhance your digital security posture. Each of these technologies is used to secure a different aspect of your digital environment:

- » **Antivirus/anti-malware:** You should always have antivirus and anti-malware software installed and have the definition files up to date.
- » **Firewalls:** All systems should have firewalls enabled, and the network should be protected by a network firewall.
- » **User authentication/strong passwords:** Ensure that users authenticate to the network before accessing resources, and mandate that they have strong passwords that are not easily guessed.
- » **Multifactor authentication:** In high-secure environments, use multifactor authentication, which involves users authenticating to a system with a combination of something they know, something they have, and something they are.
- » **Directory permissions:** Be sure to set permissions on folders and directories. This ensures that users who have authenticated to the environment don't get access to resources they shouldn't have access to.
- » **VPN:** For all users accessing the network from across the Internet, be sure they use VPN technology, as it will encrypt all communication from their computers to the office network and back.
- » **DLP:** Data Loss Protection is a technology that ensures employees are not leaking sensitive data outside the company. Be sure to look at DLP solutions to ensure sensitive data cannot be copied or emailed by employees.

- » **Disable ports:** Look to disabling ports on the switch that are not being used so that you can prevent any additional systems that may try to connect to the system without authorization.
- » **Access control lists:** Similar to an entry control roster that records physical access into and out of a facility, an access control list is a list of people who can access a folder or file on the network. An ACL is also a list of traffic that can pass through a firewall or router. Be sure to configure ACLs on both types of items.
- » **Smartcard:** Smartcards are a type of multifactor authentication. Someone using a smartcard to log onto a system must physically have the card as well as know the PIN.
- » **Email filtering:** Email filters allow you to reduce the amount of spam messages that enter into the network. (A spam message is an unsolicited message that typically is advertising a product or service from a company.)
- » **SecureDNS:** Hackers are constantly trying to alter your DNS records to lead you to the hackers' sites, so it is critical that you implement security features with DNS. You can use DNS Security Extensions (DNSSEC) to digitally sign your DNS records and add integrity to your DNS records.
- » **Trusted/untrusted software sources:** Be sure to always use software from a trusted software source, which is a company that has proven to create non-malicious software.

## *User education*

As a security professional within the organization, it is important to educate the user on security incidents that could occur if best practices are not followed. Educate users on concepts such as tailgating and social engineering attacks so that they are comfortable with how to handle such incidents.

Also educate users on password security best practices. Ensure that users know not to write down their passwords or share them with other employees, and make sure that they know how to change their password.

## *Principle of least privilege*

One of the fundamental principles of security is the principle of least privilege, which means that when you give someone permission to a resource or the rights to perform a task, ensure that you always give the minimum privileges necessary. For example, if you need Bob to change the time on the computer, you could put him in the Administrators group or you could just give him the Change System Time right. The proper choice is to give him the Change System Time right because placing Bob in the Administrators group accomplishes the goal but also allows Bob to modify every other aspect of the system.

## *Workstation security best practices*

You have a number of best practices to follow when you look at security best practices for workstations. Security best practices that relate to workstation security range from having good password best practices to good account management practices.

### *Password best practices*

To keep your workstations secure, you must follow some command password best practices. Be sure to implement the following points on your workstations in regard to password management:

- » **Requiring passwords:** Ensure that you require passwords for someone to gain access to a workstation or a mobile device.
- » **Setting strong passwords:** Ensure that passwords are complex passwords, meaning that they should contain a mix of uppercase and lowercase letters, numbers, and symbols.
- » **Password expiration:** Be sure to have passwords expire on a regular basis. The benefit of password expiration is that if a hacker figures out a user's password, or that user shares his or her password (which is not allowed) with someone else, at least the password can only be used until it expires.
- » **Changing default usernames/passwords:** All Windows systems have a username of "administrator" by default. It is important to rename that account to hide the account name and make it harder for someone to

log on as an administrator. Also be sure to set a strong password for the administrator account after you have renamed it.

- » **Screensaver required password:** Be sure to have a screen saver kick in after a small period of inactivity (5 or 10 minutes). Also make sure that a password is required to use the system after the screen saver has become active. This limits who can use the system if an employee leaves the system temporarily.
- » **BIOS/UEFI passwords:** Make sure you secure your systems by setting BIOS or UEFI passwords on the system. These passwords kick in as soon as the machine powers on and appear even before the OS loads.

### *Account management best practices*

Not only do you need to ensure you manage passwords at the workstation to help create a secure environment, but you must also follow some common account management best practices to increase security of the workstations. Following are some common account settings you should implement:

- » **Restricting user permissions:** Ensure that you are following the principle of least privilege by making sure that employees only have user-level access to the system. Employees do not need administrative access to the system.
- » **Logon time restrictions:** When configuring user accounts, you can restrict the accounts to only be able to log onto the system or network within certain times. For example, to ensure an employee does not have access to company data after working hours, you could restrict his or her login time from between 8:30 a.m. and 4:30 p.m. This typically also means the user is disconnected from the network after his or her login hours expire.
- » **Disabling guest account:** Most operating systems have a guest account that can be used to connect to the system without needing an actual username and password. Ensure that the guest account is



disabled on all systems so that a username and password are required to access the system.

- » **Failed attempts logout:** When configuring security for your user accounts, you should configure a maximum number of failed logon attempts before the account is locked and cannot be used again until the administrator unlocks it.
- » **Timeout/screen lock:** You should configure automatic timeout and screen locks on systems and mobile devices so that the device requires a password after a few minutes of inactivity.
- » **Change default admin user account/password:** It is a security best practice to modify the default account with any system. You should rename the admin account to a name not easily guessed, and be sure to modify the default password of the account.
- » **Basic Active Directory functions:** In order to allow users to log onto the network and access network resources, create a user account in Active Directory for those users. When creating the account, be sure to specify a unique password on the account and force the password to expire on a regular basis. Delete the Active Directory account if the user leaves the organization, but disable the account if the user goes on temporary leave. You don't want to delete the account if the employee is coming back at a later time because if you do, when he or she comes back, you will need to re-create the account and set up all the security again for that account. From time to time you will need to reset passwords for users who forget their passwords, and also unlock an account that has been locked due to multiple failed logon attempts.

### *Other security best practices*

Some other areas of configuration to help improve the security of your systems and environment are configuring autorun, data encryption, and patch management. The following outlines key points with each of these:

- » **Disable autorun:** If you disable autorun on the system, you have a bit of protection against an employee using a DVD with malicious

software from automatically executing.

- » **Data encryption:** You should be using data encryption technology to encrypt data on a disk. This is useful as it protects your data from someone who decides to access the drive by booting a different operating system.
- » **Patch/update management:** Patch the system and keep up to date with security updates in order to fix vulnerabilities that exist in the software on the system.

## *Troubleshooting Mobile OS and Device Security*

A big part of troubleshooting systems and security in this day and age is working with mobile devices such as smartphones and tablets. As an IT professional, you will need to troubleshoot a number of scenarios with mobile devices and ensure that the privacy of the data on the device is protected.

### *Troubleshooting mobile devices*

IT professionals are presented with a number of common issues related to mobile devices not working as expected. The following are some common scenarios you should know for the A+ exams and the real world:

- » **Signal drop/weak signal:** If the device is experiencing a loss of signal from the provider, you can go into the network settings and choose to reconnect. If this doesn't work, try a hard reboot.
- » **Power drain:** If you notice the power draining on the device, you may need to replace the battery. Before taking that big step, you could experiment first by ensuring apps are closed down if not being used. Also, you could try disabling wireless in times when you are not using wireless as the device may be constantly working to find wireless networks.

- » **Slow data speeds:** If experiencing slow data speeds, you may need to refresh the tower list on the mobile device. This is a common procedure that the mobile network provider will walk you through when experiencing dropped connections or slow data speeds.
- » **Unintended WiFi connection:** If you connect automatically to a wireless network you are not expecting, you could go to the wireless network list and clear the WiFi settings for a particular WiFi network. This will prevent automatically connecting to that network.
- » **Unintended Bluetooth pairing:** If connecting to an unintended Bluetooth device automatically, you could go into the Bluetooth settings on the device and remove the pairing settings of that Bluetooth device so that your mobile device does not automatically connect to it.
- » **Leaked personal files/data:** To prevent data leaks from your device, be sure to follow common mobile device security procedures such as password-protecting the device, having the device auto lock after a short period of inactivity, and encrypting the data on the device.
- » **Data transmission over limit:** To prevent going over data limits, you can control what apps are allowed to use your data plan. In this situation, set critical apps such as email to use your data plan, but maybe require WiFi to surf the Internet via a browser. You may also have data-saver settings on the device that once enabled will do things like not download an image sent to you until you click the image to view it.
- » **Unauthorized account access:** You should look at the permissions applications have on your mobile device and restrict what an application can access.
- » **Unauthorized location tracking:** Ensure you control which applications can access GPS location tracking services on the device.
- » **Unauthorized camera/microphone activation:** Ensure you monitor which applications have the capabilities to activate your microphone and camera on your mobile device.
- » **High resource utilization:** Most devices give you a summary of the resources used by different applications such as data and battery

power. From this information you can decide if you want to uninstall certain applications or restrict the resources they can use.

## *Device security*

More and more business users are doing much of their communication and work on mobile devices. This means your company security policy should specify how those devices should be secured in order to prevent data theft and data leakage. The following are some common practices around device security:

- » **Password protection:** Ensure your device requires a PIN or password before someone can access the device.
- » **Auto lock:** Configure the device to automatically lock after a short period of inactivity. This will ensure that if you leave the device on a desk, someone cannot pick it up and gain access to sensitive information. A password is needed in order to gain access after the device auto-locks.
- » **Device encryption:** Ensure the device is encrypting the data stored on the device. For laptop computers, ensure that the hard drive is encrypted with full disk encryption technology such as Bitlocker.
- » **Remote wipe:** For company assets, ensure you have the capability to remotely wipe (erase) a device that is lost or stolen. This will ensure that if someone has your device in his possession, there is no data on the device.
- » **Device location services:** Some devices allow you to track their locations. This allows you to locate your device with its GPS services if it is lost or stolen.

## *Introduction to Incident Response*

*Incident response* is how you respond to security incidents within the organization. It is critical that you have an incident response procedure in place so that when a security incident occurs, employees know how to

report the incident and the security officers know how to handle the incident.

A *security incident* could be an employee noticing that her account has been locked out, a system that has been infected with a virus, or a user receives a phishing email, or it could be related to a user accessing prohibited content or performing prohibited activity on the network. You will respond to each of these incidents in different ways.

## *The first response*

Although each type of incident will be handled in a different way, the overall process is similar with all security incidents. Handling a security incident starts with the first responder. The role of the first responder is as follows:

- » **Identify:** The first step in handling an incident is to identify that the incident has occurred and to contain that incident. For example, when looking at logs, you notice that Sue has been surfing inappropriate content, so you contain the incident by blocking her system from Internet access.
- » **Report through proper channels:** When an incident has been identified, all employees should understand how to report the incident. For example, an end user should know whom he should report a security incident to as well as to the network administrators. Typically, the user may report a problem to the network administrator, and upon looking into the problem, if the network administrator notices that the problem is security related, he would notify the security officer within the company.
- » **Data/device preservation:** The goal of containment is to prevent the security incident from becoming a bigger problem, but you are also trying to preserve the state of the system. For example, if the system was hit with a virus, you would disconnect the system from the network to prevent the system from infecting the rest of the network. But if you noticed that the system was hacked into, you are disconnecting the system from the network to prevent the hacker from having continued access to the system. Disconnecting the system can

prevent the hacker from destroying logs on the system along with other important data on the device.

## ***Documentation***

When responding to problems or security incidents, you can typically solve a lot of recurring problems by looking to problem-solving documentation systems. Most large companies log all problems including security incidents so that when a problem arises, the administrator troubleshooting the problem can search the documentation system for related problems. If a match is found, the documentation can give the responder a number of steps to perform to respond to the incident.

If the company invests in a documentation system to help solve problems, it is important to train all administrators on how to record problems and solutions into the system. You also need to ensure that the administrators are updating the documentation as new problems arise or different solutions are found to existing problems. The documentation system is useless without the documentation!

## ***Tracking of evidence/chain of custody***

When responding to incidents, it is important to collect evidence of the incident. The evidence could be an employee's mobile device such as a phone or laptop, or it could be log files on a web server. When you collect the evidence, you must "bag and tag" the evidence and store it in a secure location at all times. You should also document all your activity as you respond to the incident, as you may need to explain the steps you took to respond to the incident or discover evidence.

It is critical that you track the evidence location at all times so that you validate the integrity of the evidence. When collecting the evidence, have forms that are filled out describing the evidence and label the bag with an evidence ID number.

The most critical part of collecting evidence is to have a *chain of custody* document that lists where the evidence was at all times. If someone takes the evidence out of the secure location to review it, he must fill out the

chain of custody to indicate when he took the evidence, when it was returned, and where it was at all times.

## *Licensing*

Employees using unlicensed software on company systems and devices may also be the source of security incidents within the organization. It is important to have a security policy that covers the company's rules surrounding the usage of unlicensed software and ensure employees know what software is authorized for use.

When it comes to software licensing there are a few key points you should keep in mind:

- » **DRM/EULA:** *Digital Rights Management* (DRM) is a set of technologies that are designed to protect digital assets from unauthorized use. For example, using DRM, a movie rental company can have a movie file expire two days after it is downloaded. In a company setting, with DRM, a company can ensure that employees cannot forward an email. The *End User Licensing Agreement* (EULA) is a contract between the software vendor and the user of that application that specifies rules of use for the software. For example, the EULA may specify that the user is not allowed to redistribute the application or reverse engineer it.
- » **Open source versus commercial licenses:** An *open source license* is a license that allows the source code of an application to be freely downloaded, modified, and redistributed. A *commercial license* applies to software that has been created by a company that typically sells the software. The commercial license typically puts restrictions in place that limit modifications to the software and redistribution of the software.
- » **Personal license versus enterprise licenses:** A *personal license* of software typically allows a user to install the software once on a system using a license key. An *enterprise license* is typically a license to install the software on a specific number of systems within the corporation.

## *Regulated data*

Regulated data refers to personal information such as identification data, health records, or credit card data. In most cases, when it comes to processing and storing sensitive information, you need to ensure the data is encrypted. That way if unintended users access to the data, they would only see the encrypted version of the data because they would not have the encryption key to decrypt and view the sensitive information. The following are types of data that have regulations specifying how companies must protect the data:

- » **PII:** Personally Identifiable Information (PII) is information about a person that can uniquely identify that person over any other person. Examples of PII are social insurance numbers, social security numbers, license plate numbers, and driver's license numbers. Depending on the industry your organization works in, you may be controlled by regulations that dictate how PII is to be stored and secured.
- » **PCI:** Payment Card Industry (PCI) data is data from a credit card that is used by an application. When storing information from a credit card, you should encrypt the sensitive data such as the credit card number. PCI data security standards state that other information about the card such as the name and expiration information associated with the card does not need to be encrypted as long as the card number is.
- » **GDPR:** A European standard known as General Data Protection Regulations (GDPR) requires organizations that handle personal data put security controls in place to protect an individual's personal data.
- » **PHI:** Protected Health Information (PHI) is health information records about a patient that must be safely guarded.

## *Corporate policies*

A company must have a security policy in place that dictates the security posture of the company. It is important that all employees are familiar with the security policies of the company and that they follow these corporate policies. It is also important to make sure that employees



understand what happens if policies are not followed. Corrective action could be loss of a company device such as a mobile phone, or even employee dismissal.

## Getting an A+

This chapter introduces you to a number of security-related terms that you need to understand before taking the A+ exams. Here some key points to remember when preparing:

- » *Authentication* is the process of proving an identity to the network, but *authorization* is the process of determining whether accessing a resource is allowed after authentication takes place.
- » Hackers take many different approaches to compromise a system. Protect your environment from both network-based and software-based attacks, and make sure that physical security is in place.
- » A *denial of service* (DoS) is an attack on a system or network that prevents the system or network from performing its regular function.
- » *Social engineering* is a popular type of attack that involves the hacker compromising security by tricking an employee through social contact. The social engineer might entice the user to divulge confidential information or might trick the user into running a program that does harm to the system.
- » You secure network traffic by *encrypting* traffic between two systems by using technologies such as SSL and IPsec. Administrators typically use SSL to encrypt web traffic and IPsec to encrypt internal or VPN traffic.
- » Securing your data involves not only protecting resources with permissions but also protecting your data by following proper data destruction procedures and backup strategies as well as creating redundant disk solutions.

## Prep Test

- 1. Susan calls you over to her desk to tell you about an awkward phone call she just received. The caller claimed to be the administrator and asked her to reset her password in order to enable access to a new piece of software being deployed. What type of attack potentially just occurred?**
  - (A) Password attack
  - (B) Eavesdrop attack
  - (C) Man-in-the-middle attack
  - (D) Social engineering attack
  
- 2. One of the network technicians for the company is using a packet sniffer to see if she can view confidential information traveling over the network. What type of attack is this?**
  - (A) Password attack
  - (B) Eavesdrop attack
  - (C) Man-in-the-middle attack
  - (D) Social engineering attack
  
- 3. What type of attack involves the hacker causing your system or network to become unresponsive to valid requests?**
  - (A) DoS attack
  - (B) Eavesdrop attack
  - (C) Man-in-the-middle attack
  - (D) Password attack
  
- 4. You are the server administrator for your company and want to implement a form of RAID that duplicates the data fully on two disks. Which RAID solution would you use?**
  - (A) Striped volume
  - (B) Mirrored volume
  - (C) RAID 5 volume
  - (D) RAID Level 0

- 5. Your manager is concerned that the batch of new laptops purchased for the sales team will be stolen in no time at all. What should you purchase for each laptop to help protect it from theft?**
- (A) Flash drive
  - (B) Driver disk
  - (C) A Doberman Pinscher
  - (D) Lockdown cable
- 6. Your manager is looking to increase the authentication system by using biometrics. Which of the following are forms of biometrics? (Select all that apply.)**
- (A) Fingerprint scan
  - (B) Smart card
  - (C) Username and password
  - (D) Retinal scan
- 7. You are a server technician for your company, and you are planning your backup strategy for data stored on the server. What type of backup copies the files that have changed but does not clear the archive bit?**
- (A) Full backup
  - (B) Incremental backup
  - (C) Differential backup
  - (D) Copy
- 8. What technology is typically used to encrypt traffic between a web server and web browser?**
- (A) DoS
  - (B) IPSec
  - (C) Smart card
  - (D) SSL

**9. You are a technician at a company. Your manager has been reading about tailgating in a recent security article and asks you what the company can do to prevent tailgating. Which of the following would you recommend?**

- (A) Lockdown cable
- (B) Mantrap
- (C) Degaussing tool
- (D) Key fob

**10. Your manager would like to look at increasing the security posture of the company by implementing multifactor authentication. Which of the following combinations represent multifactor authentication?**

- (A) Smartcard and PIN
- (B) PIN and password
- (C) Username and password
- (D) Retina scan and fingerprint

## *Answers*

1. **D.** Social engineering is a type of hack that involves contacting victims through phone or email and tricking them into doing something that compromises company security. See “[Social engineering attacks](#).”
2. **B.** An eavesdropping attack occurs when a hacker monitors network traffic to try to capture information that could be useful in another attack. Review “[Eavesdropping attack](#).”
3. **A.** A denial of service (DoS) attack is when a hacker consumes all the system’s processing power or bandwidth so that it cannot perform its normal job. Check out “[Denial of service](#).”
4. **B.** A mirrored volume is used to create a full duplicate of the data on two different disks. Peruse “[Implementing RAID solutions](#).”

5. **D.** A lockdown cable is used to secure the laptop to a desk to help prevent the laptop from being stolen. Refer to “[Understanding Physical Security](#).”
6. **A, D.** Biometric devices involve authenticating a user through the user’s unique physical characteristics. Fingerprint scans and retinal scans are popular biometric authentication methods. See “[Authentication](#).”
7. **C.** A differential backup backs up only those files that have changed since the last full backup and then does not clear the archive bit. Check out “[Backup review](#).”
8. **D.** Secure Socket Layer (SSL) is used to encrypt web traffic. You can identify whether you are on a secure website by looking for the lock icon at the bottom of the screen. Inspect “[Methods of Securing Transmissions](#).”
9. **B.** A mantrap is used to prevent tailgating. A mantrap is an area between two locked doors with the second door not opening until the first door is closed. Peruse “[Understanding Physical Security](#).”
10. **A.** To be considered multifactor authentication, the authentication system must use a combination of something you know, something you have, and something you are. A smartcard is something you have, and a PIN is something you know. Scrutinize “[Multifactor authentication](#).”

# Chapter 2

## Implementing Security

---

### IN THIS CHAPTER

- » Securing systems through BIOS
  - » Implementing users and groups
  - » Implementing permissions and rights
  - » Implementing auditing
  - » Implementing firewalls
  - » Implementing security best practices
- 

In this chapter, you find out how to implement security best practices on systems at home or at the workplace. The preceding chapter introduces terms such as *authentication* and *authorization*; this chapter demonstrates how to perform such tasks. You find out how to create a user account that can be used for authentication and how to authorize the user to access a folder or perform an action within the operating system. This chapter will ensure that you know how to perform basic security-related tasks!

When thinking about network security, understand that security is to be implemented at multiple layers, meaning that you cannot focus on just one security-related feature. You want to implement multiple security features to secure your environment. For example, a number of people feel that their systems are secure because they have a firewall. They don't realize that the firewall protects the system only from attacks coming across the network. What if the hacker is in the same room as the computer? The firewall is of no use at that point, so you need to ensure that you implement other security features to protect the system from all potential threats.

# *Securing Systems through BIOS/UEFI*

When securing systems, your first security concern is physical access. This involves ensuring that critical systems, such as servers, are in locked rooms that are not accessible to unauthorized users. Physically securing systems could also involve changing some of the CMOS settings, such as boot device order, power-on password, and CMOS password.

Changing these settings in CMOS is different for each type of system, but the first thing to do is enter CMOS. Normally, you press Delete, F1, F2, or F10 when the system is booting.

After the system is booted, you will find the following settings in the CMOS setup program to help secure the system:

- » **BIOS Password:** Usually found in the security section of CMOS, you can set a power-on password (also known as a user password), which is a password that anyone who wants to use the system must type. You may also set an admin password, which is a password that must be known by anyone who wants to change CMOS settings.
- » **Boot Devices:** In CMOS, you can control what devices the computer can boot from. Most computers today can boot from DVD-ROM, hard disk, network, and USB removable drives. It is important to understand that if you allow a computer to boot from DVD-ROM, a hacker can possibly boot from a DVD and bypass all security enforced by your operating system.
- » **Intrusion Detection:** Most systems today have an intrusion detection option that will notify you if the computer case has been opened. This is important because instead of stealing the actual computer, a person could take the RAM or hard drive out of the computer, which is easier to hide and steal. Make sure that the intrusion detection option is enabled, and also be sure to lock the computer cases so they cannot be removed easily.

# *Understanding Logical Security Concepts*

Understanding security concepts is the key to creating a more secure environment. In this section you learn about logical security concepts that all add to the overall security of the organization when implemented.

## *Authentication concepts*

A key concept to implement in any environment where security is a concern is authentication. *Authentication* involves verifying the identity of someone trying to access a system or network. When looking at a stand-alone computer, you typically authenticate against the local security database of a system, but in a corporate network environment, you typically authenticate against a network account database. Once you log on with a username and password, a security token is assigned to you, and that token is then used to determine if you get access to resources on the network. This is known as *single sign-on*, where the one username and password is used to access multiple systems on the network.

Another important point to remember about authentication is *multifactor* authentication. Multifactor authentication is common today with cloud-based services where you want to add a layer of security to your account. Instead of just requiring a username and password, accounts are configured to send a text message with an access code to a user's phone. This way, if someone is logging on with your username and password, she must have your phone in her possession in order to know the access code (which changes with every logon).

## *Active Directory terminology*

The most common single sign-on environment is Active Directory. In an Active Directory environment, you log onto what is known as a *domain*. A domain is a group of computers that all work in the same security boundary, with the logon request being answered by the domain controllers. Domain controllers are the types of servers that store the



network account database of usernames and passwords (known as the Active Directory database).

The user accounts in Active Directory have a few common properties — the accounts can have a *logon script* assigned, which is a script that executes every time the user logs on. This script usually sets up items such as mapped drives. When users log on they also can have *group policies* applied to them or updated. A policy is responsible for restricting what the user can do on a system or network, and also setting configuration settings on that system. For example, a group policy may configure a feature known as *folder redirection*, which is when a folder such as the Documents folder is redirected to a server. The end result is that the users think they are saving files to the local Documents folder, but the files are actually being saved to the server.

In Active Directory, the user accounts are organized into *organizational units*. These are containers that are used to hold similar user accounts in the same area of Active Directory. Once you organize your users into organizational units, you can then apply group policies to the organizational units in order to apply the same restrictions to those users.

A *home folder* is another setting that is applied to user accounts. Each user has a personal folder on the network which is configured as a setting on that user's account. This allows users to store files in a location that only they can access the files (and potentially the administrators).

## ***Controlling access***

Once users have authenticated to the network, you can then control what they have access to. There are a number of different technologies that are used to control access on the network:

- » **Software tokens:** When you log on, an access token is generated in the background and associated with everything you do on the network. This access token contains items such as your user ID, groups you are a member of, and any special rights you have been given. This token is then presented to any servers you try to access on the network to determine if you are allowed to access the resources on that server.

- » **MDM policies:** Mobile Device Management (MDM) policies control what mobile devices the user can use to access the network. The mobile device is then controlled by the MDM policies with features such as device encryption and password requirements for the device.
- » **Port security:** Port security is a feature of network switches that allows you to control what devices are allowed to plug into which ports on the switch. This allows you to control who can physically connect to the network.
- » **MAC address filtering:** Many technologies such as wireless allow you to control which devices are allowed to connect to an asset by the MAC address of the network card of a device.
- » **Certificates:** You can also control access to resources such as files and folder by using certificates — an electronic file that contains your private key.

You learn about *principle of least privilege* in Book 9, [Chapter 1](#), but I wanted to mention it again here because it is an important security principle when discussing access control. When giving someone access to a resource, be sure to give the minimum permission needed — that is the principle of least privilege.

## *Implementing Users and Groups*

In this section, you find out how to create user accounts that can be used to log on to the system and how to create groups to organize users together as a single object that permissions can be assigned to.

### *Creating user accounts*

To secure the Windows OS from unauthorized access, you can create a user account for each person who is allowed to use the system. Anyone without a user account will be unable to log on to the system and, as a result, will not be able to use the computer. The other benefit of creating user accounts is that even if a person has a user account and logs onto the system, he might not be able to access a file because you have not given permission to that user to access the file.

## Creating accounts in Computer Management

To create a user account on a Windows system, go to Control Panel ⇒ Administrative Tools ⇒ Computer Management. In the Computer Management console that opens, expand Local Users and Groups and select the Users folder (shown in [Figure 2-1](#)). In the Users folder, you will notice some user accounts on the right side. These user accounts are *built-in accounts*, meaning that they were built by the OS or by a piece of software you have installed. Note that the home editions of Windows do not have a Computer Management console, so you will have to manage user accounts through the Control Panel.



**FIGURE 2-1:** Creating user accounts and groups in the Computer Management console.

Two built-in accounts you should be familiar with for the A+ exams are

- » **Administrator:** The *administrator account* is the built-in account in Windows that has full access to the system and can manage all aspects of the computer. During the installation of Windows, you were asked what you wanted to set as the password for the administrator account;

you use that password to log on with the username of `administrator`. When you do log on as administrator, you can change any settings on the system. A normal user account cannot change major settings on the system such as the time, installing software, or any changes that affect the system. To make these types of changes, you need to log on as administrator to make changes.

- » **Guest:** Users can use the *guest account* if they don't have an actual user account. When they try to access the system, they are authenticated as `guest`. The guest user inherits any permissions the guest account has on the system. There is one hook to this scenario, though. By default, the guest account is disabled, meaning that it is not available for use. Because of the security concerns of not requiring someone to log on, Microsoft has disabled the account. A disabled account appears with a red X on it and cannot be used.



FOR THE  
EXAM

Two default accounts are built in to Windows: administrator and guest. The administrator account has full access to the system, and the guest account is used for temporary access to the system. Also note that the guest account is disabled by default.

Now that you have identified the two major built-in accounts, you can create your own user accounts. To create your own user accounts in the Computer Management console, right-click the Users folder and choose New User. The New User dialog box appears (shown in [Figure 2-2](#)). Fill in the following account details:

- » **User Name:** This is the name that the user uses to log on to the system. Typically, it is a short version of the full name. For example, the full name Glen Clarke might get truncated to `gclarke` as the username. A username is also known as the *logon name*.
- » **Full Name:** This is typically the person's first name and last name: for example, `Glen Clarke` as the full name.

- » **Description:** This is a description of the user account. I typically put the person's job role here: for example, `Accountant`.
- » **Password:** Type what you want for the user accounts password. The user needs to know this password to log on to the system. Be sure to use good practices with passwords, such as not using words found in the dictionary and using a combination of uppercase and lowercase letters, numbers, and symbols. See the preceding chapter for more information about strong passwords.
- » **Confirm Password:** Type the password again in this box. This ensures that you typed what you thought you typed.
- » **User Must Change Password at Next Logon:** Set this option if you want to force the user to change the password the first time he logs on. This ensures that you don't know the user's password because the password you originally set is overwritten.
- » **User Cannot Change Password:** Set this option if you don't want the user to be able to change the password. This ensures that the password you set is the password that the user must use.
- » **Password Never Expires:** In a password policy, you can specify that passwords must be changed every so many days. That policy applies to all users except for any accounts that have Password Never Expires activated. You might use this option if you have two employees sharing a user account.
- » **Account Is Disabled:** If you want to disable an account at any time, you can set this option. A disabled account is unusable until you enable it again.

The image shows a 'New User' dialog box from a Windows operating system. The title bar at the top says 'New User' and includes a help icon (?) and a close icon (X). The dialog box contains the following fields and options:

- User name:** bsmith
- Full name:** Bob Smith
- Description:** Accountant
- Password:** [masked with dots]
- Confirm password:** [masked with dots]
- ☒ User must change password at next logon
- ☐ User cannot change password
- ☐ Password never expires
- ☐ Account is disabled

At the bottom right, there are two buttons: 'Create' and 'Close'.

**FIGURE 2-2:** Creating a user account in Windows.

After you enter all the account information, click the Create button and then click Close to dismiss the New User dialog box. The user account has been created, and you can start using it right away to log on to Windows.

### *Creating accounts in Control Panel*

It is also possible to create user accounts from within the Control Panel. In Windows 7, click User Accounts from the Control Panel and then select Family Safety ⇒ User Accounts ⇒ Manage Another Account. At this point you can select a user account you want to alter or create a new user account by choosing the Create a New Account link.

In Windows 8.1, you can also manage user accounts from the Control Panel by selecting User Accounts and Family Safety ⇒ User Accounts ⇒ Manage Another Account ([Figure 2-3](#)). Choose the account you want to alter and then choose the action on the left side that represents the change to the account you want to make. If you want to create a new account, click the link for Add a New User in PC settings from the Manage

Another Account screen. This takes you to the PC settings screen where you can add a new user account.



**FIGURE 2-3:** Creating a user account via Control Panel.

One user account setting you can change is the type of account. In Windows you can create a *standard user* account (the default), which is just a plain account with no administrative permissions. You can also create an Administrator account, which has permissions to alter settings on the computer.

To change the account type after the fact, simply go to Control Panel ⇒ User Accounts and Family Safety ⇒ User Accounts ⇒ Manage Another Account, and then select the account you want to alter. On the left side of the screen you will see settings you can change. Choose Change Account Type and then choose either Standard User or Administrator.

## *Creating groups*

A *group* in Windows is a collection of user accounts. The benefit of using groups when managing access to resources is that you don't need to assign the same permissions multiple times. Instead, you assign the permission to the group, and anyone who is a member of the group receives the permission.

Like user accounts, Windows offers a number of built-in groups. A built-in group has predefined capabilities within Windows. For example, printer operators can manage all printers on the system, and anyone who

is a member of the printer operators group will have that capability. The following is a list of some of the popular built-in groups found in Windows OSes:

- » **Administrators:** This group has full access to the system and can change any setting on the system. The administrator account is a member of this group by default, which is why the administrator account is allowed to change any setting on the system.
- » **Backup Operators:** Members can perform backups and restores on the system.
- » **Account Operators:** Members can create user accounts. This group is available on Windows servers. The benefit of using this group is that if you want someone to be able to manage user accounts, you can place that person in this group instead of in the administrators group and he or she will only be able to manage the user accounts — not the entire system.
- » **Printer Operators:** Members can change any settings on the printers. Essentially, members of this group are trained to troubleshoot the printing environment and then assigned the task of managing all printing problems on the network.
- » **Users:** All user accounts that are created are members of the users group. You can assign permissions to the users group knowing that all users will get the permission.
- » **Power Users:** The power users group is the group on Windows client OSes prior to Windows Vista that allows its users to create user accounts and manage the printing environment. Use this group if the desktop OS does not have an account operator or a printer operator group.



FOR THE  
EXAM

Be sure you know the default groups in Windows. Some of the more useful built-in groups are account operators, printer operators,



and backup operators. Also note that if a user is not placed in an administrative group, he or she is known as a *standard user*.

If the built-in groups do not satisfy your needs, create your own groups:

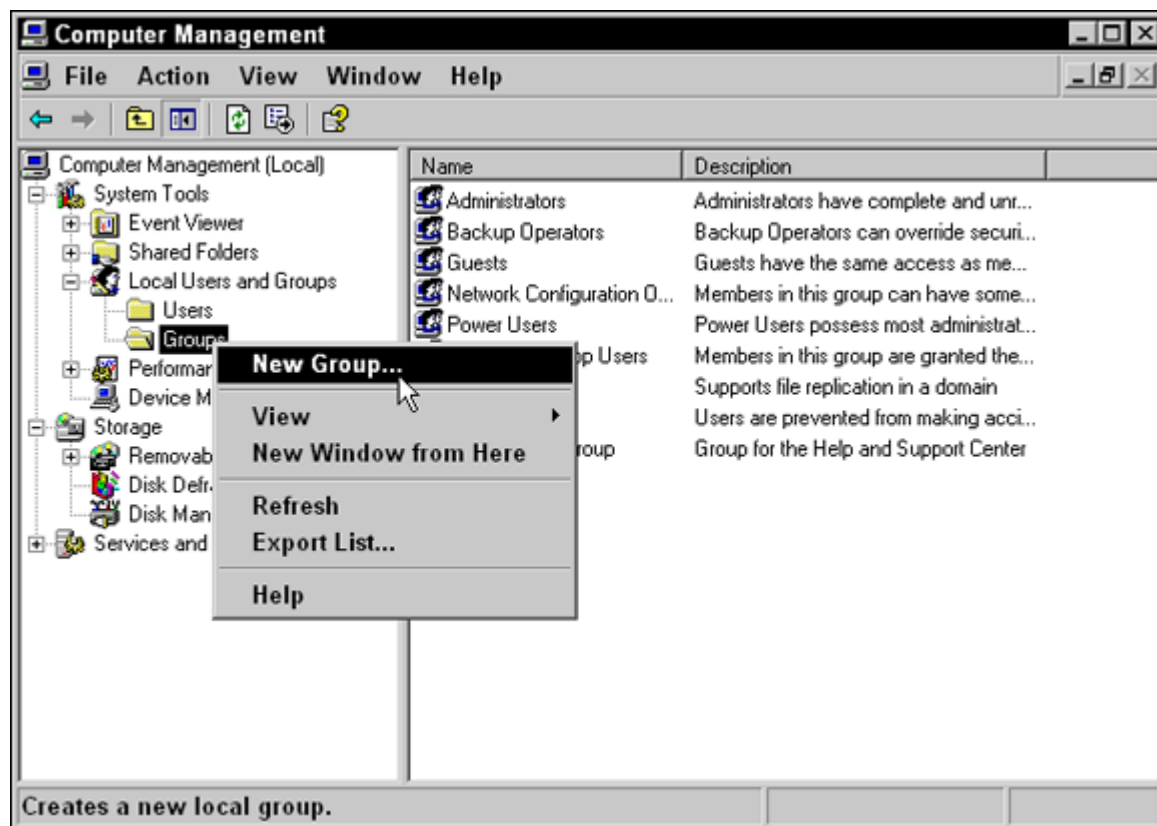
1. **Click Start and then right-click Computer (in Windows 7 and Vista) and choose Manage. In Windows 8.1/Windows 10, right-click the Start icon and choose Computer Management.**
2. **In the Computer Management console, expand Local Users and Groups.**
3. **Right-click the Groups folder in Local Users and Groups and then choose New Group, as shown in [Figure 2-4](#).**
4. **In the New Group dialog box that appears, type the name you want to use for the group.**

In this example, I use Accountants (shown in [Figure 2-5](#)).

5. **Fill in a description for the group in the Description text box.**
6. **To begin adding members to the group, click the Add button.**  
The Select Users dialog box appears.
7. **Type the name of the user account you want to add and then click the Check Name button on the right side.**

Windows should underline the account name, indicating that the user account exists and that you can add it to the group membership.

8. **Repeat Step 7 for each account you want to add to the group.**
9. **After you add all the accounts to the group, click OK and then click Create to create the group.**



**FIGURE 2-4:** Creating a new group in Computer Management.



**FIGURE 2-5:** Fill in information for your new group.

After you create the users and place them into their appropriate groups, you are now ready to assign them permissions.



ON THE  
WEB

To practice creating users and groups, take a look at Lab 2-1 on the book's companion website at [www.dummies.com/go/aplusaio](http://www.dummies.com/go/aplusaio).

## *Implementing Permissions and Rights*

When controlling a user's access to the system, you typically modify the user's *rights* and *permissions*. Microsoft has made a huge distinction between a permission and a right.

- » **Permission:** A user's level of access to a resource, such as a printer or file
- » **Right:** A user's privilege to perform an OS task

In this section, you discover the difference between permissions and rights within the Windows OS and how to implement both within the local security policy in Windows.

### *User rights*

If you were to log on to your Windows system as just a user account and then double-click the time in the bottom-right corner to change that time, you get an error message indicating that you do not have the privilege to change the time. This is an example of user rights. The user account that you are currently logged in with does not have the right to change the system time, which is an action that typically has to be performed by an administrative account.

There is a large list of user rights; some of the most popular ones are listed below:

- » **Access this computer from the network.** This right is needed by anyone who wants to connect to the system from across the network: for example, if you want to connect to a shared folder on computer A, you need to this right on computer A.
- » **Back up files and directories.** This right is needed by anyone who wants to back up files on the computer. For security reasons, not everyone should be able to perform backups on a system, so Windows controls who can perform a backup via this right.
- » **Change the system time.** To change the time on the computer, your user account must be given this right.
- » **Log on locally.** To log on to the system by pressing Ctrl+Alt+Delete, you need this right. Microsoft classifies *a local logon* as you sitting in front of the computer at the keyboard (versus a *remote logon*, where you connect from across the network, which is controlled by the first right mentioned in this list).
- » **Shut down the system.** To shut down the computer, you must have this right.
- » **Take ownership of files and other objects.** In Windows, the owner of the object, such as a file or folder, always has the ability to change the permissions of the resource. You might want to give selected individuals the take-ownership right so that they can take ownership of a resource and then change the permissions.

To change the user rights (for example, to assign Bob Smith the right to change the system time), you need to modify the user rights assignments in the local security policies of the Windows computer. The local security policy controls all security settings for the system. To change the local security policies in Windows, follow these steps:

1. **In Windows 7, choose Start ⇒ Control Panel. In Windows 8.1, right-click the Start icon and then choose Control Panel. In**

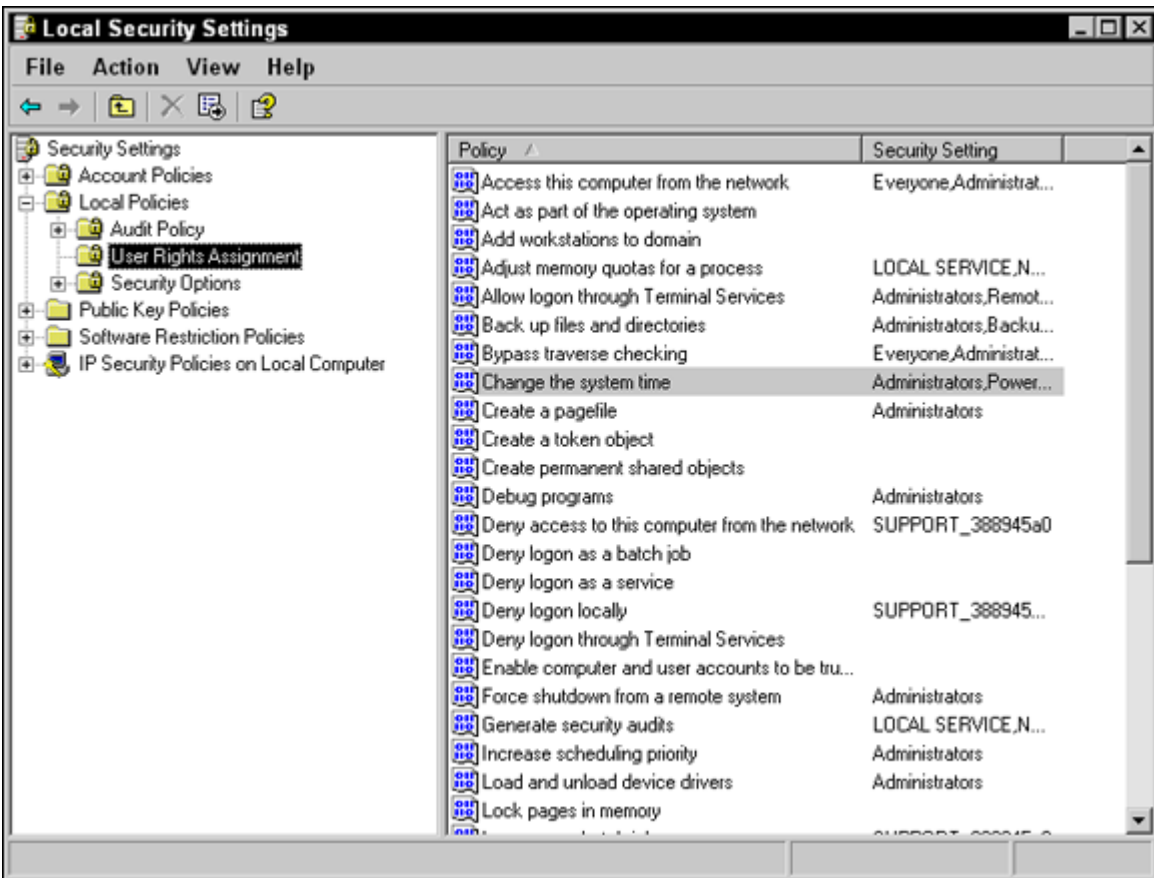
**Windows 10, click the Start button, type control, and then choose Control Panel from the menu.**

- 2. In the Control Panel, choose System and Security and then Administrative Tools.**
- 3. In the Administrative Tools, double-click Local Security Policy to start the Local Security Policy console.**
- 4. To modify the user rights within the local security policy, expand Local Policies and then highlight User Rights Assignments, as shown in [Figure 2-6](#).**

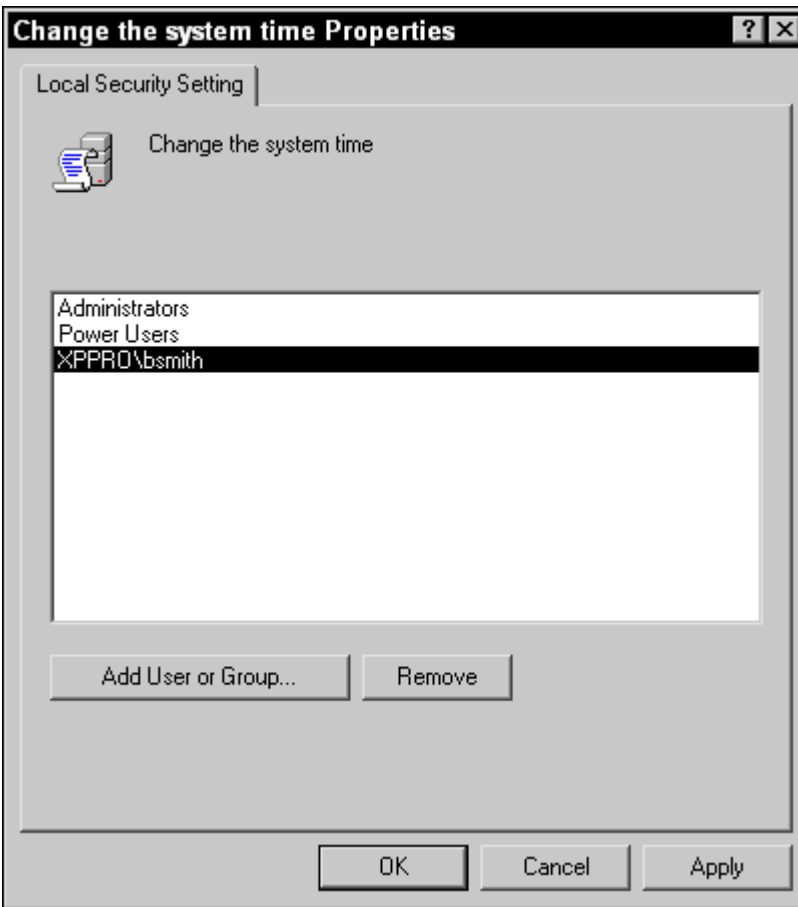
When the User Rights Assignments node on the left side has been selected, you will notice the list of user rights on the right side of the screen in the Details pane.

- 5. To modify a user right, double-click the user right.**

You see a list of users or groups that have been assigned that right.
- 6. To add a user or group to the list, click the Add User or Group button, type the name of the account you want to add, and then click Check Names to ensure that Windows recognizes the user account.**
- 7. Click OK to add the account to the right you chose (as shown in [Figure 2-7](#)) and then click OK to close the window.**



**FIGURE 2-6:** Configuring user rights within Windows allows you to control which actions a user can perform on that computer.



**FIGURE 2-7:** Adding Bob to the change the system time user right.

## *User Account Control (UAC)*

Starting with Windows Vista, Microsoft added the *User Account Control* (UAC) feature, which was improved in Windows 7. When an administrative account logs onto Windows, that user is not initially given administrative access to the system. When the administrator launches a program to perform some administration, Windows prompts the user to raise the privilege level to the administrative level. If the administrator chooses Continue, Windows then elevates the user's privileges to the administrative privileges.

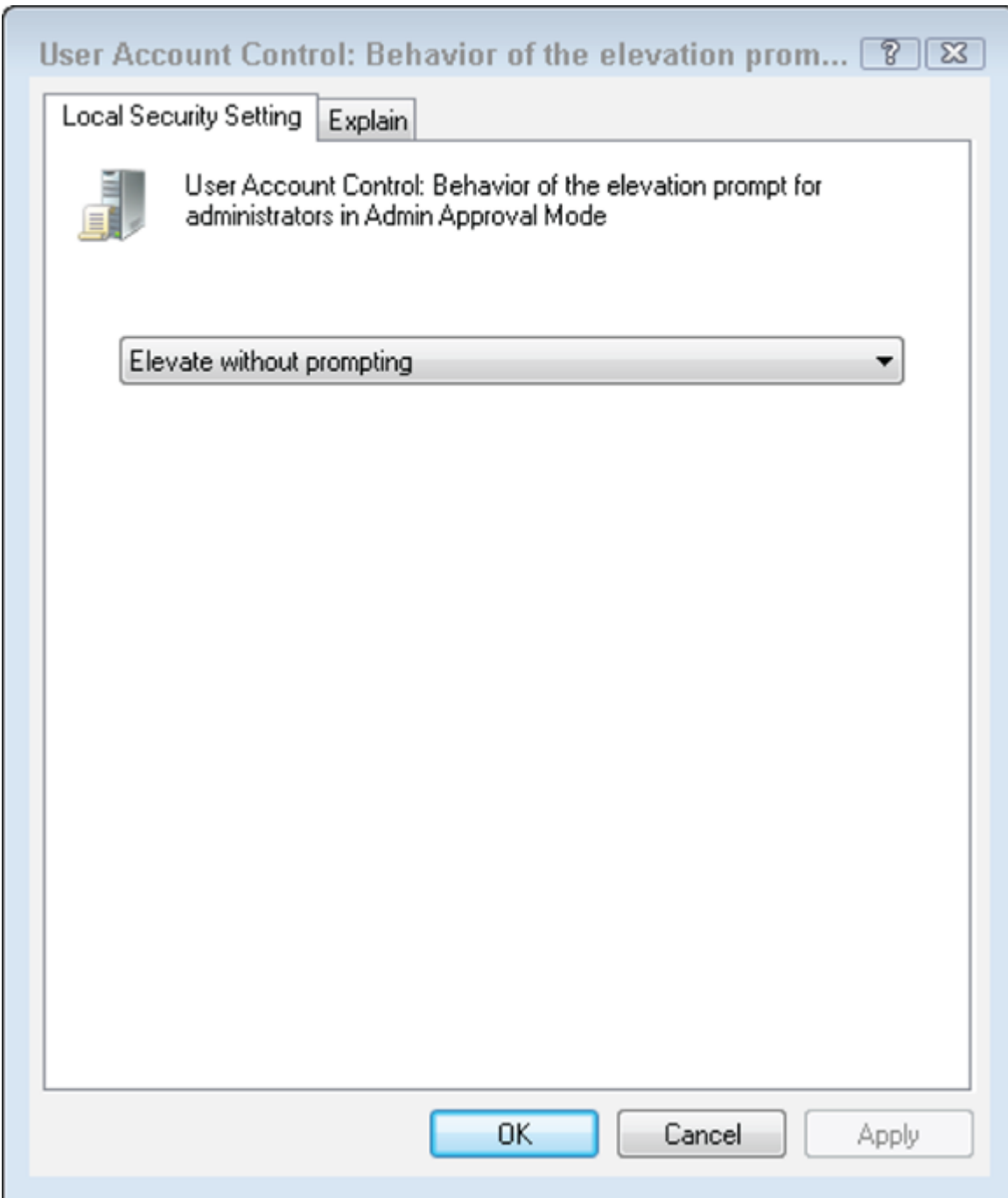
Microsoft created the feature because over the last few years, a number of security incidents were caused by hackers that caused the user of the computer to run malicious software without the user's knowledge — and because the user logged on had admin access to the system, so did the

program that the user did not know was running. This malicious software that now had admin access could do anything it wanted to the system.

In response, Microsoft created the UAC feature. Now if software runs without your knowledge and tries to manipulate the system, you are prompted to decide whether you want to continue. Unfortunately, you also get prompted when you launch the software yourself, which is why most people get frustrated with the UAC feature. Still, it is a great feature from a security point of view.

You can modify the local security policy to get rid of the UAC prompt and automatically elevate the admin privileges (not recommended). Locate the User Account Control: Behavior of the Elevation Prompt for Administrators in Admin Approval Mode setting in the Security Options section of the Local Policy. You can set the value of the policy to Elevate Without Prompting, as shown in [Figure 2-8](#).

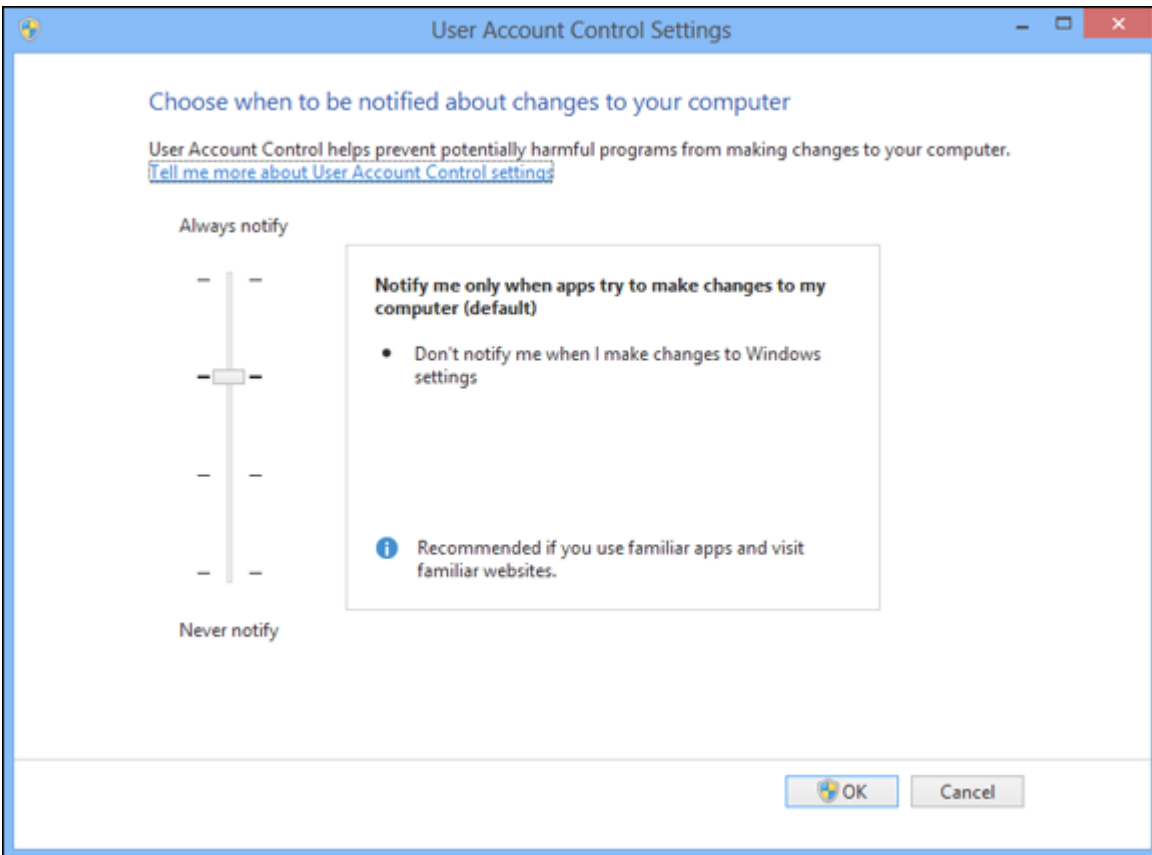




**FIGURE 2-8:** Modifying the UAC feature within the Local Security Policy.

You can also change how the UAC feature works in Windows via the Control Panel (instead of the security policy). To change the UAC settings through the Control Panel, select User Accounts and Family Safety ⇒ User Accounts, and then choose the Change User Account Control Settings link. A dialog box appears that allows you to control when you get the

notifications about elevating your privileges (see [Figure 2-9](#)). The default is to notify you when a program tries to make a change, but not notify you when you make a change. If you want to remove all notifications, drag the slider to the bottom to the Never Notify setting.



**FIGURE 2-9:** Modifying the UAC feature via Control Panel.

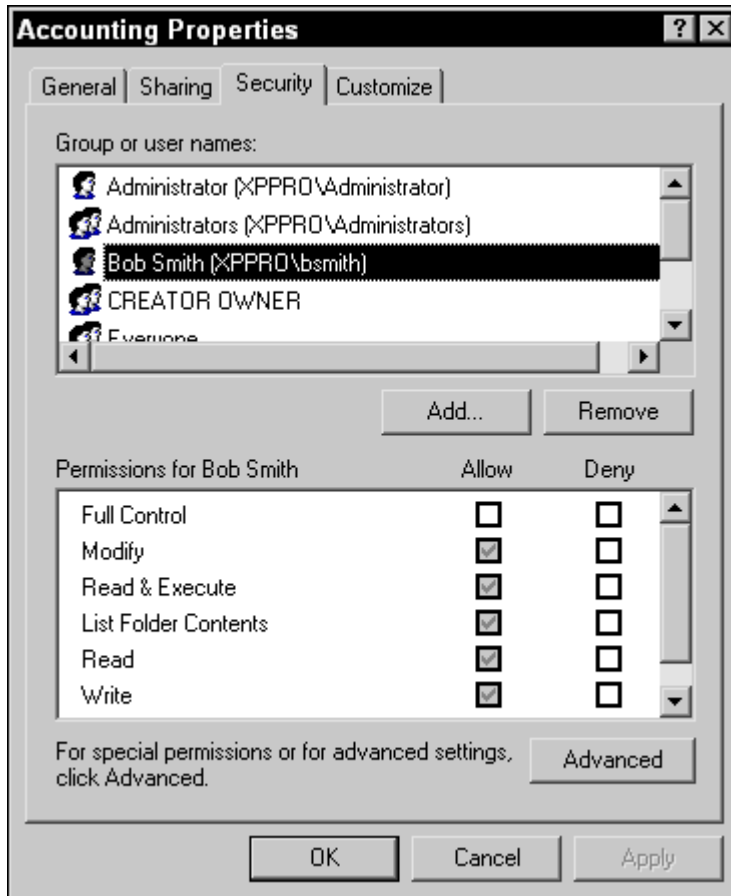
## RUN AS ADMINISTRATOR VERSUS STANDARD USER

Another feature you should be familiar with is the fact that as you launch software on the system, even if you are an administrator of the system, the software is launched with standard user privileges. This means you will not be able to make changes to the system using that program.

If you know that you are launching the software in order to make changes to the system, then you can right-click on the program and choose Run As Administrator. If you are logged in already with an administrative account, your privileges will be elevated while you are running that software. If you are not logged in as an administrator, you will be prompted for the username and password of an administrative account.

## Permissions

Permissions are different than rights: A right governs an action that can be performed on the computer, but a *permission* is a user's level of access to a resource. For example, you can give a user permission to read or modify a file. [Figure 2-10](#) shows the permissions you can set for a file.



**FIGURE 2-10:** Looking at NTFS permissions in Windows.



TECHNICAL  
STUFF

Permissions can be configured only on a partition formatted for NTFS. To obtain an NTFS partition, you can format the partition for NTFS (but lose all existing data), or you can convert the drive to NTFS by using the `convert driveletter: /fs:ntfs` command. When you convert, the existing data on the drive is preserved.

To modify the permissions on a folder or file in Windows, simply right-click the file or folder and choose Properties. In the Properties window, choose the security page tab to set the permissions.

Here are the available permissions:

- » **Read permissions:** What I call the “read” permission is a combination of the three default permissions — Read, Read and Execute, and List Folder Contents. I personally classify all three as the read permission because at a minimum, this is typically what users need to read the file.
  - *Read:* Allows you read the contents of a file
  - *Read and Execute:* Allows you to read the contents of the file and execute a program
  - *List Folder Contents:* Allows you to see the file when you look in the folder
- » **Modify:** Allows a user to read, modify, and delete a file. When given the Modify permission to a folder, a user can also create new files or folders in that folder.
- » **Full Control:** Allows a user to do everything that the Modify permission allows, and the user can also change permissions on the resource or take ownership of the resource.



**WARNING** If someone can take ownership of the resource, that person can change the permissions. The Full Control permission should be used sparingly so that not everyone has the permission to change permissions on you.

- » **Write:** Used by the Modify permission to allow users to write to the file or folder. When you choose the Modify permission, you will notice that the Write permission is automatically selected.

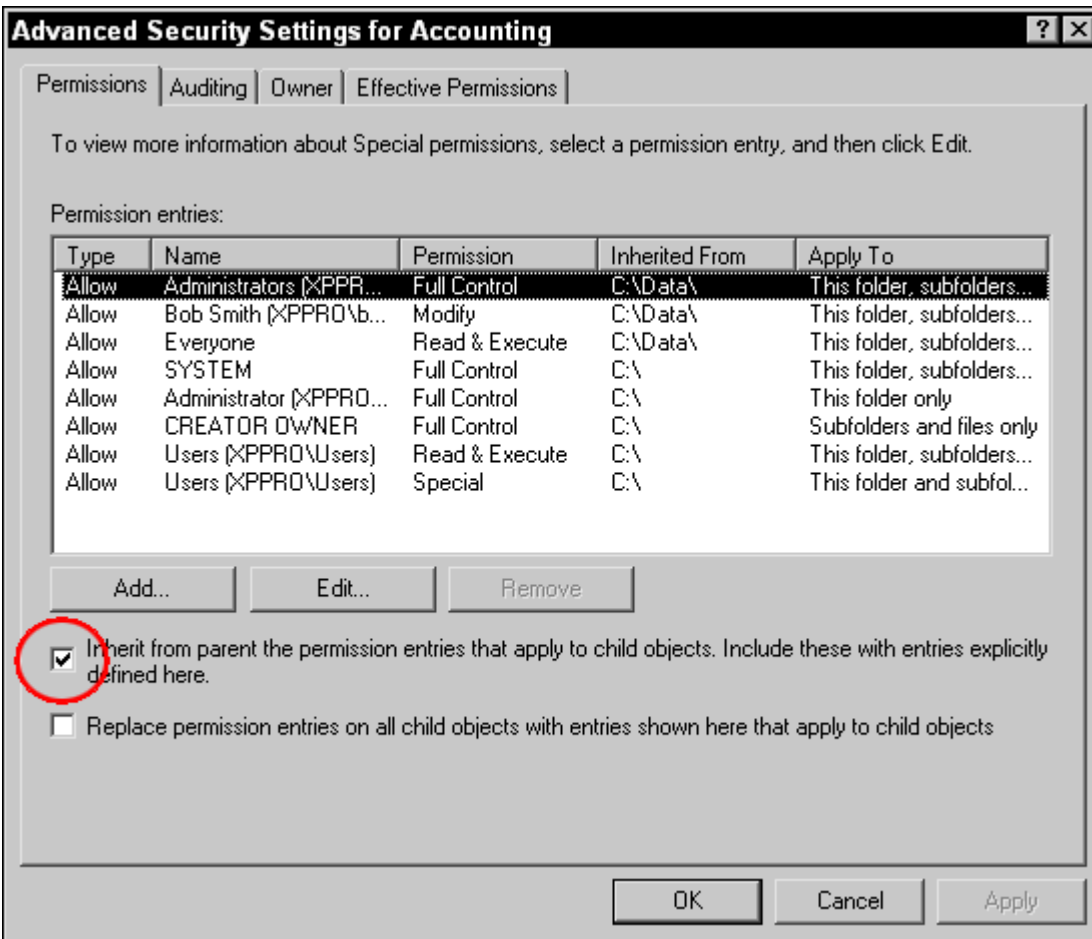


FOR THE  
EXAM

The major difference between the Modify permission and Full Control permission is that Full Control allows a user to modify permissions and take ownership of the resource in addition to being able to modify and delete the resource.

Looking at [Figure 2-10](#), you will notice a number of permissions with gray check boxes next to them. The gray check box means that you are not allowed to change the permission because the permission is being inherited from a parent level. *Permission inheritance* (also known as *permission propagation*) is a feature of Windows that is designed to minimize how much permission management you need to do. With permission inheritance, when you set permission on a folder, that permission applies to all subfolders and files; you don't need to go to subfolders and files to set the same permission.

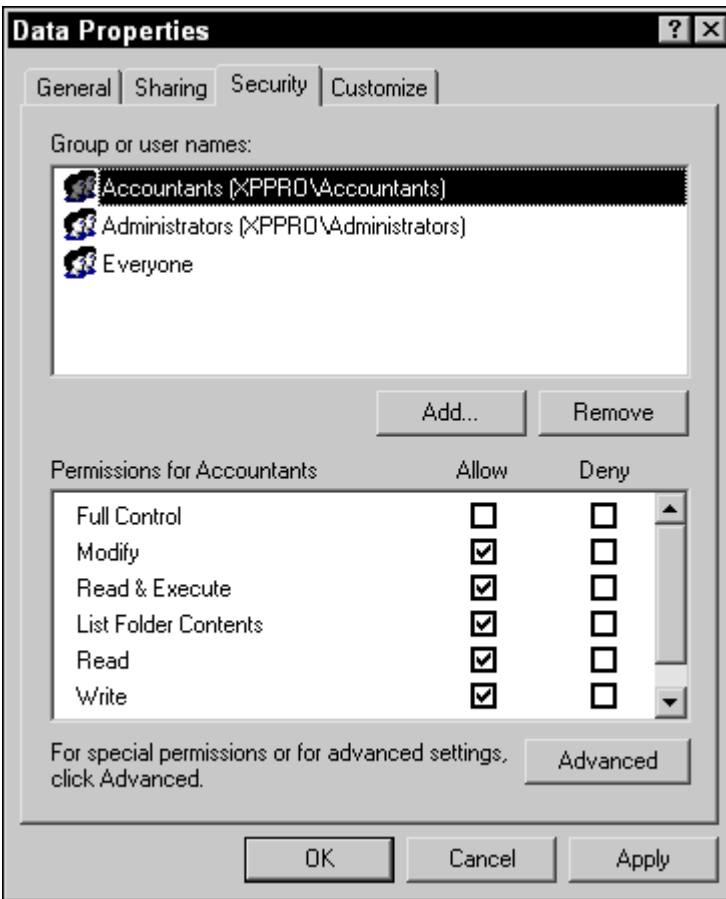
When you go to modify the permissions on a folder, however, you need to understand that the existing permissions are being inherited from the parent folder. To change the permissions, you need to break the permission inheritance feature on the folder by going to the properties of the folder, clicking the Security tab, and clicking the Advanced button. That invokes the Advanced Security Settings dialog box for the folder, where you can turn off the Inherit from Parent option (see [Figure 2-11](#)).



**FIGURE 2-11:** Disabling permission inheritance in the Advanced Security Settings dialog box.

After you turn off the inheritance option and click OK to close that screen, you are presented with a dialog box asking whether you want to remove the existing permissions or copy the permission down from the parent folder so that you do not have to set all permissions again. Typically, I choose Remove and then add whoever needs to have access to the folder.

After you remove the existing permissions, you can add new users or groups to the permission list on the Security tab by clicking the Add button. You can type the name of the account or group you want to assign the permission to and then click the Check Names button. After you add all the users and groups to the permission list, you then choose which permission you want assigned to each user by selecting the user in the permission list and then choosing the permission. For example, in [Figure 2-12](#), notice that the Accountants group has the Modify permission.



**FIGURE 2-12:** Giving the accountants the Modify permission.



**ON THE  
WEB**

To practice changing permissions and rights, take a look at Lab 2-2, which can be found on the book's companion website at [www.dummies.com/go/aplusaio](http://www.dummies.com/go/aplusaio).

### ***Allow versus deny***

Note that the descriptions in this chapter have been about allowing a permission such as the modify permission. From time to time, you may want to take someone's permissions away with a *deny* permission. A reason to do this would be if the user is a member of a group that has been allowed a permission and you do not want the user to have the permission; you simply add the user to the access control list and deny him the permission! All users in the group will be allowed the permission

except for that one user. Remember that in Windows, the deny permission wins over an allow permission when a conflict occurs.

### *File attributes*

You can change the attributes of a file and make it read-only so that no one can modify the file, or you can make it hidden so that no one can see the file. These are not great practices as far as security goes because when setting a file attribute, it applies to everyone. For example, if you set the read-only attribute on a file, the file cannot be modified by anyone, including users and administrators. With permissions, you get to choose who gets the permission.

### *Copying and moving files*

Permissions on a file can change as you perform file management tasks, such as moving and copying files. The following list shows the outcome if you move or copy a file that has permissions set on it:

- » **Move on same partition.** When you move a file from one folder to another folder on the same partition, the file keeps its permissions.
- » **Copy on same partition.** When you copy a file from one folder to another folder on the same partition, the new file inherits the permissions of the folder that it was copied to.
- » **Move across partitions.** When you move a file from one folder to another on different partitions, the file inherits the permissions of the target folder and does not retain its original permissions. This is because when you move a file between partitions, Windows first copies the file and then deletes the original (if the copy was successful).
- » **Copy across partitions.** When you copy a file from one partition to another partition, the new file inherits the permissions of the destination folder.





FOR THE  
EXAM

Remember the effect that copying and moving files have on the permissions of the destination file.

### *NTFS versus share permissions*

When you share a folder, you have the opportunity to place permissions on the share, as well as to set up your NTFS permissions. (Book 8, [Chapter 3](#) covers sharing network resources such as folders and printers.) The big question is what happens when the two permissions conflict? If a conflict in permissions between NTFS and shared folders exists, the most restrictive takes effect. For example, if you have NTFS permissions of modify on a folder and then you share the folder and give all users the read permission, the permission that takes effect will be the read permission because it is the most restrictive. Remember this for your A+ certification exams!



**REMEMBER** The share permission is inherited for the entire folder structure of the share, which is known as *permission propagation*. Also, remember that administrative shares are already created in Windows, such as the root of every drive. You can connect to them with syntax such as `\\computername\c$`, but remember that only administrators can connect to administrative shares!

### *Shared files and folders*

You learn about shares in Book 8, [Chapter 3](#), but let's do a quick review of the key points here and focus on security-related facts you need to know about shares (on top of what you just read).

The purpose of sharing a folder is to ensure that users from across the network can access those files. Once you share the folder, the share is given a name, and users on the network will connect to that folder using the UNC path of `\\servername\sharename`.

## *Administrative shares versus local shares*

There are two types of shares in Windows: administrative shares and local shares. Administrative shares are default folders that are already shared by Windows, but the permissions on the administrative share are configured so that only administrators can connect to the share. An example where an administrator may use an administrative share is if he or she needed to connect to the root of the drive on the server to copy some files from the server. The roots of all drives are administrative shares by default.

In Windows, the following are default administrative shares:

- » **Admin\$:** The Admin\$ share is a hidden administrative share that references the Windows folder, typically `c:\windows`.
- » **IPC\$:** The IPC\$ administrative share is used by programs that need to communicate with the system.
- » **<DriveLetter>\$:** The most common administrative share is the fact that the root of each drive is shared on the system, allowing an administrator to access the entire drive remotely. An example of accessing this share would be `\\servername\c$`.

Not only do we have administrative shares, but administrators can also create local shares. A local share is a folder that is manually shared by the administrator of the system.

## *Configure shares*

You learn how to share a folder in Book 8, [Chapter 3](#), but let's review the steps to share a folder. To share a folder in Windows 8.1, follow these steps:

1. **Locate the folder you want to share on your system.**
2. **Right-click the folder and choose Share With ⇒ Specific People.**
3. **In the File Sharing dialog box, choose the user (or group) you want to share the folder with from the drop-down list, and then choose Add.**

#### 4. Choose the Permission Level for the share:

- *Read*: Allows the user or group to read files from the share folder but not make changes to the content of the shared folder.
- *Read/Write*: Allows the user or group to add a file to the share and modify or delete his or her own files.
- *Owner*: Gives the user full permission to the share, including modifying and deleting any files in the share.

#### 5. Click the Share button.

#### 6. Click Done.

### *System files and folders*

From a security point of view, you should be familiar with where the system files and folders are for the operating system and ensure that you do not give users unnecessary access to these folders. The Windows operating system is stored in the `c:\windows` directory, with many of the files being stored in `c:\windows\system32`. Other examples of folders that store files used by the system are `c:\program files` and `c:\program files (x86)`. Be sure to limit who has access to those folders.

## *Implementing Auditing*

After you set up security on a Windows system by setting permissions on the folders and files, configuring user rights, and placing users in the appropriate groups, make sure that the security of the OS is effective. To monitor what is happening on the system, you enable auditing, which notifies you when certain things happen on the system. For example, you might want to be notified if someone fails to log on to the system, using a correct username and password — this could be someone trying to guess the password of the account.

To effectively work with the auditing feature in Windows, there are two steps:

### 1. **Enable auditing.**

You must first enable auditing. Simply choose what events you want to audit. The nice thing about auditing in Windows is that you choose which events you care to know about.

### 2. **Review the audit log.**

After you enable auditing, ensure that you monitor the log regularly for any security-related issues. For example, if you notice a failure to log on over and over for the same account, that is an indication that an account is being hacked.

The following sections offer more details about these two steps.

## ***Enabling auditing***

To enable auditing in Windows, modify the Local Security Policy:

1. **In Windows 7, choose Start ⇒ Control Panel. In Windows 8.1, right-click the Start icon and choose Control Panel. In Windows 10, click the Start button, type control, and choose Control Panel from the menu.**
2. **In the Control Panel, choose System and Security and then Administrative Tools.**
3. **In the Administrative Tools, double-click Local Security Policy to start the Local Security Policy console.**
4. **In the Local Security Policy console, expand Local Policies and then highlight Audit Policy.**

On the right side of the screen (the Details pane) is a list of events for which you can enable auditing (see [Figure 2-13](#)):

- *Audit Account Logon*: Audit any remote users who are authenticated by this user account database. This is the event to enable auditing on a domain controller.



TECHNICAL  
STUFF

A *domain controller* is a server in a Microsoft network environment that holds all the user accounts for an entire network. In the corporate world, users log on to the network, not a particular machine, which means that the logon request is sent to the domain controller where the username and password are checked against a database. The database that holds the user accounts on a domain controller is known as the *Active Directory* database.

- *Audit Account Management*: Record an event in the log for any user account changes, such as any new accounts that are built, modified, or deleted.
- *Audit Logon Events*: Record the fact that the user logged on from this station regardless of whether the account was authenticated from this system.
- *Audit Object Access*: Audit access to a specific folder, file, or printer.



TIP

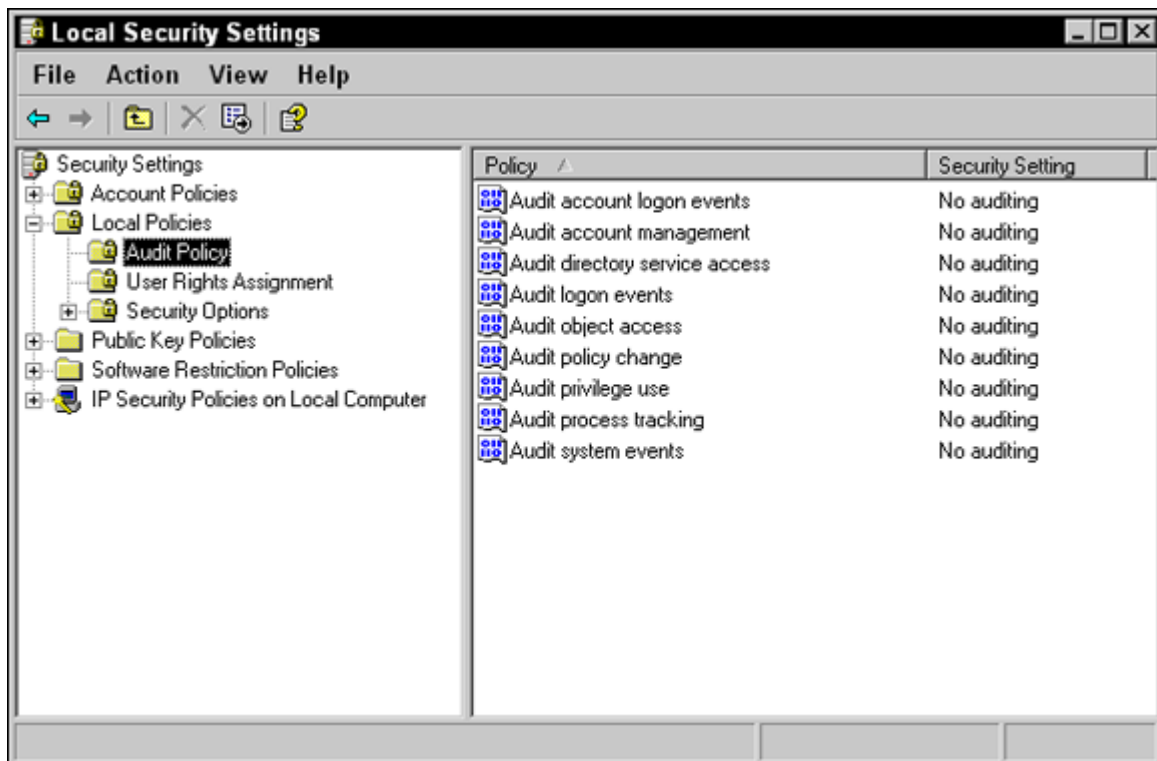
After you enable Object Access Auditing, you need to go to the Security page in the properties of a file, folder, or printer and click the Advanced button. Click the Auditing tab and choose which users and which permissions to audit for. You must perform this step on any folder, file, or printer you want to audit.

- *Audit Policy Change*: Notification of any change to the security policy.
- *Audit Privilege Use*: Logs when a user takes advantage of any rights you have given that user. For example, if you give Bob the right to perform backups, you want to know when he actually performs a backup.

- *Audit Process Tracking*: Notification of when a process starts or exits.
- *Audit System Events*: Notification of system-related actions, such as restarting or shutting down the system. You might want to be aware when the system is restarted, especially on server OSes.

5. To enable auditing on one of these events, double-click the event and then choose whether you want to audit the success of that event or the failure.

For example, I do not care about the success of logons, so I would choose Failure for that event.



**FIGURE 2-13:** Looking at the auditing feature within the Local Security Policy.

## *Reviewing the security log*

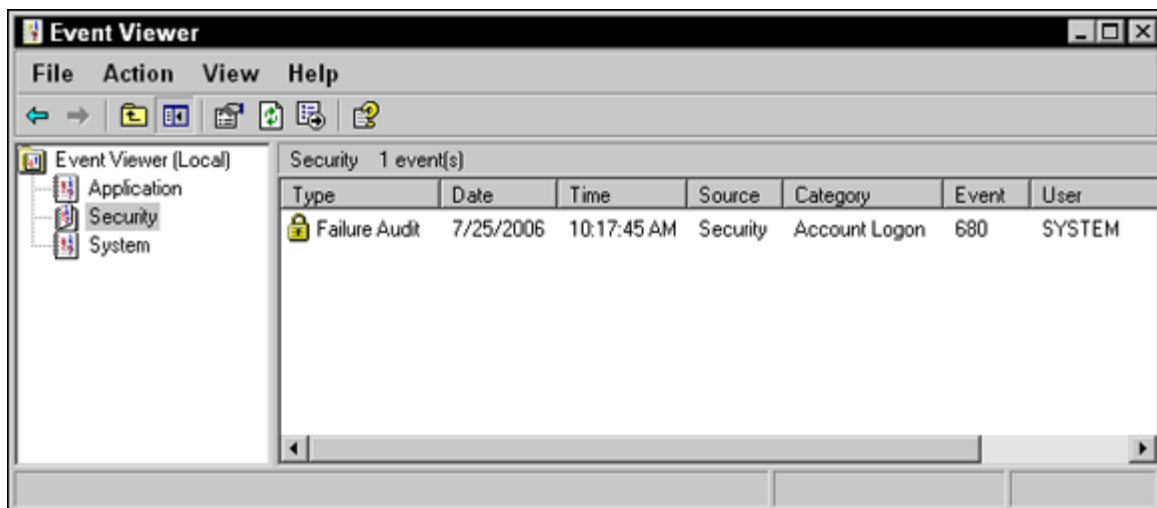
After you enable auditing on the different events, you then need to view the audited information in the security log of event viewer:

1. In Windows 7, choose Start ⇒ Control Panel. In Windows 8.1, right-click the Start icon and choose Control Panel. In Windows 10, click the Start button, type control, and choose Control Panel from the menu.
2. In the Control Panel, choose System and Security and then Administrative Tools.
3. In the Administrative Tools, double-click the Event Viewer to start the Event Viewer console.
4. On the left side, expand Windows Logs and then select the log that you want to view.

Note the events on the right side of the screen. If you select the security log, as shown in [Figure 2-14](#), any events with a lock are failure events, and any events with a key are successful events. [Figure 2-14](#) shows an account logon event with a lock, indicating a failure to log on.

5. (Optional) To view a description of a particular event, double-click the event.

Going back to the account logon failure example, you can see the date and time the logon was attempted. You can also view the username that was attempted and the computer that the person used to try to log on to the network.



**FIGURE 2-14:** Review the security log that is populated by the auditing feature of Windows.



FOR THE  
EXAM

After enabling auditing, review the security events by checking out the Security log in Event Viewer.

## *Implementing Firewalls*

A *firewall* is software or hardware designed to stop information from reaching your system unless you selectively choose certain pieces of information to pass through. This information is sent in the form of network packets (pieces of data) that are broken down into three parts:

- » **Header:** Contains address information, such as source and destination addresses.
- » **Body:** Contains the packet data, known as the *payload*.
- » **Trailer:** Contains checksum information, which is a value calculated off the data in the packet and helps ensure that the data has not been tampered with or damaged in transit. If the receiving system calculates a different value based on the data it receives, and that calculated value is different than the checksum value, the receiving system knows that the data has been altered in transit.

### *How a firewall works*

A firewall is designed to look at the contents of the packet — specifically, the header information — to decide whether the data should be allowed into the system or discarded. The firewall uses the source and destination IP addresses from the header, as well as the port number, to help make this decision. A port number represents an application that runs on the system. For example, the web server installed on my system runs at my IP address on port 80. The FTP server I am also running on my system uses my IP address but uses port 21 instead of port 80. If I want to allow the public to see my website but not my FTP site, I configure the firewall to allow information to reach port 80 but not port 21. So each TCP/IP



application that is running on your system uses a different port number, which is how data is sent to one application and not the other.

My point is that the firewall also uses the port number to decide whether the data should be allowed into your system. For example, I have a website at [www.glenecclarke.com](http://www.glenecclarke.com) so I had to configure my firewall to allow data destined for port 80 to be allowed in. Now, I don't have an FTP server, so I ensured that the firewall disallows data destined for port 21.



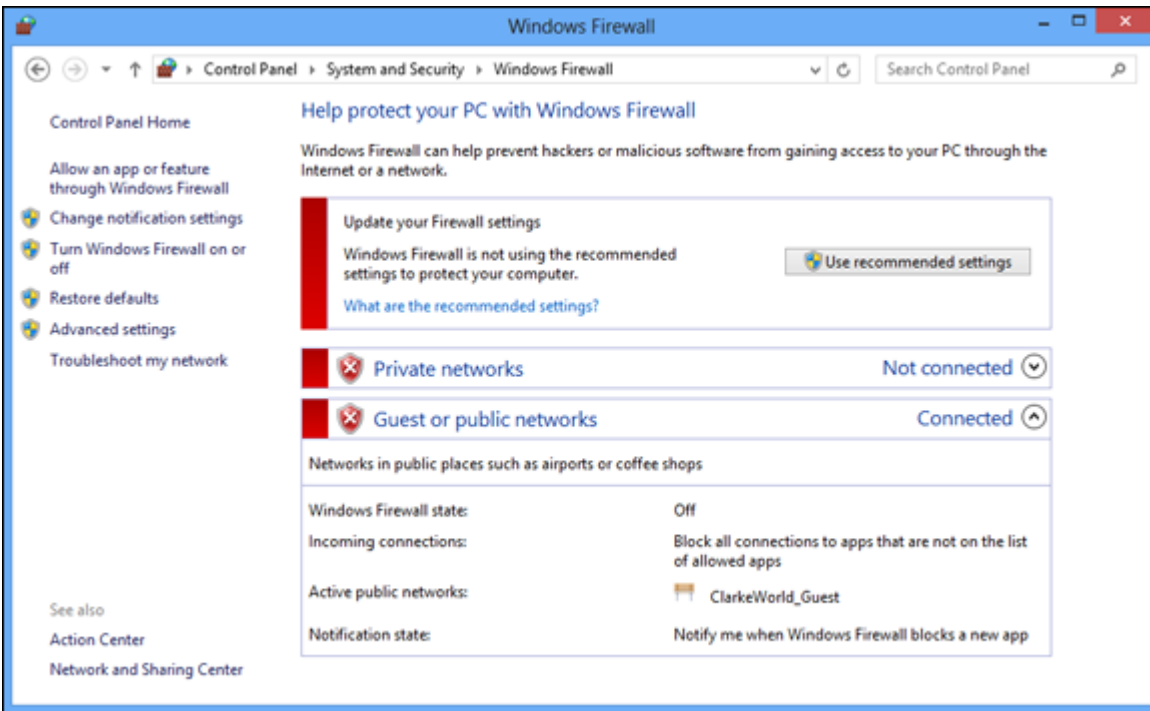
**TIP**

Understand that you don't need to open ports on the firewall unless you are hosting your own servers. For example, you don't need to open ports on the firewall to surf the Internet because most firewalls are built to allow responses to data you requested to come back through the firewall.

To enable the Windows Firewall, follow these steps:

- 1. In Windows 7, choose Start ⇒ Control Panel. In Windows 8.1, right-click the Start icon and choose Control Panel. In Windows 10, click the Start button, type control, and choose Control Panel from the menu.**
- 2. In the Control Panel, choose System and Security and then Windows Firewall (see [Figure 2-15](#)).**

You will notice a green check mark on the screen, stating that the Windows Firewall is turned on, or red squares indicating the firewall is off. You can also see the status of On or Off in the Windows Firewall state.
- 3. If the firewall is not turned on, click the Turn Windows Firewall on or off link (refer to [Figure 2-15](#)).**
- 4. You can then turn on the Windows Firewall for each network location or turn the Windows Firewall off if you like (not recommended).**



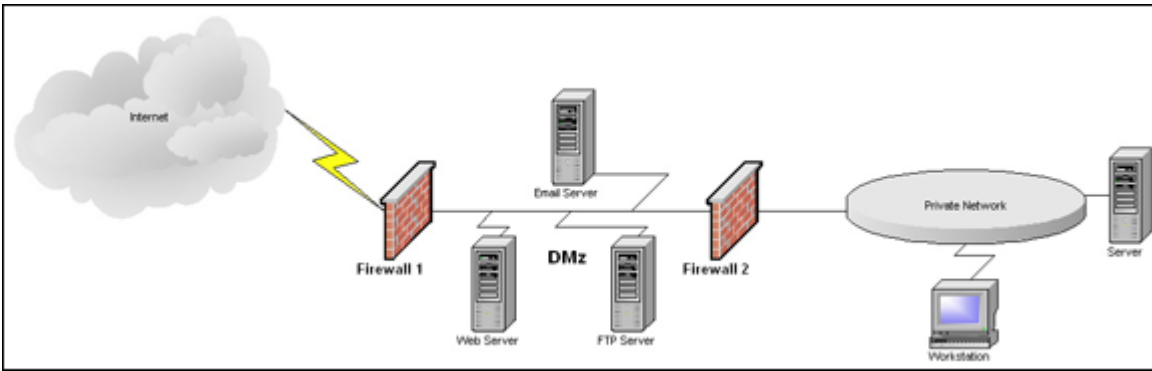
**FIGURE 2-15:** The Windows Firewall in Control Panel.

## *Creating a DMZ*

Most companies that want to publish their own websites or host other types of servers (such as FTP servers or email servers) need to allow traffic to reach these types of servers. Placing public servers such as these alongside your private network servers is unrealistic because it means that you need to open the firewall to allow traffic into the network to reach these servers.

As a work-around, most network administrators create a *demilitarized zone* (DMZ) to hold these servers. A DMZ is a network segment between two firewalls where you have allowed selected traffic to reach the servers in the DMZ. The DMZ is different from your private network because you will not allow any content to come into your private network.

[Figure 2-16](#) displays a typical DMZ setup. Note the two firewalls: firewall 1 and firewall 2. Firewall 1 connects the DMZ to the Internet and will allow only traffic destined for the three servers in the DMZ to pass through the firewall. The second firewall (firewall 2) is designed so that no systems from the Internet can pass through it, essentially protecting the private company network from outside access.



**FIGURE 2-16:** Identifying a DMZ.



**FOR THE  
EXAM**

Servers that you want to expose out to the Internet should be placed in a DMZ so that you can selectively choose which type of data is allowed to reach your servers.

## *Hardware versus software firewalls*

There are hardware firewall solutions that are physical devices placed on the network between the clients on the network and the Internet. The benefits of using hardware firewalls are that they typically outperform a software firewall, and you get the extra security benefit of having a separate security device between you and the Internet. Too, a hardware firewall solution typically protects the entire network and not just one system. Software firewalls have the benefit of being much cheaper than a hardware firewall.

### *Hardware firewalls*

A number of vendors make hardware firewalls; for example, Cisco offers the Cisco ASA firewall device. You can also use your home router as a firewall; home routers have firewall features that allow you to control what traffic is allowed to enter your network.

### *Software firewalls*

*Software firewalls* are applications installed on your computer that protect only that computer. So-called *personal firewall software*, this

kind of firewall protects only your personal computer: the one with the firewall software installed.

A number of different software firewall solutions are available. For example, Zone Alarm is a free software firewall that you can download and install on your system. Each operating system will typically have its own firewall software built-in as well. For example, Linux has iptables, and Windows has the Windows Firewall. Because most operating systems have built-in firewall software, you will most likely not need to download and install any other software.

### *Port security and exceptions*

When configuring the firewall, you typically specify rules that control which packets are allowed or not allowed to enter the network. A default rule that you typically set first states “Drop all packets” or “Accept all packets,” and then you build a list of exceptions to that default rule.

For example, on my network, I have the default rule to drop all packets, but then I have an exception that says if traffic is destined for port 80, allow that traffic into the network. This way, people on the Internet can reach my website.

To configure exceptions in Windows, follow these steps:

- 1. In Windows 7, choose Start ⇒ Control Panel. In Windows 8.1, right-click the Start icon and choose Control Panel. In Windows 10, click the Start button, type control, and choose Control Panel from the menu.**
- 2. In the Control Panel, choose System and Security and then Windows Firewall.**
- 3. Choose the Allow a Program or Feature through Windows Firewall link, located on the left side of the screen.**

You can then select the type of traffic that is allowed to pass through the firewall. For example, if you want to allow Remote Desktop into the system, choose the check box for Remote Desktop to open the RDP port on the firewall (which is TCP port 3389).

If the program you want to allow traffic through does not exist in the list, you can add an exception to the list.

4. **(Optional) To add an exception for an application or a type of traffic not in the list, click the Allow another Program button.**
5. **Select the program you want to allow to communicate through the firewall and choose Add.**
6. **Click OK and close all Windows to exit the Control Panel.**

In Book 8, [Chapter 3](#), you read more about the firewall in Windows. Within the Control Panel ⇒ System and Security ⇒ Windows Firewall dialog box, you can choose Allow a Program or Feature through Windows Firewall. If you need more flexibility, you will need to add exceptions through the Windows Firewall with Advanced Security. Here you can add exceptions by port values.

### ***Windows Firewall with Advanced Security***

If you need full control of the firewall in Windows and the capabilities to create firewall rules (exceptions) that control both inbound traffic and outbound traffic, you need to use the Windows Firewall with Advanced Security tool. Let's walk through an example of opening a port on the firewall by creating our own rule:

1. **In Windows 7, choose Start ⇒ Control Panel. In Windows 8.1, right-click the Start icon and choose Control Panel. In Windows 10, click the Start button, type control, and then choose Control Panel from the menu.**
2. **In the Control Panel, choose System and Security and then Windows Firewall.**
3. **Choose Advanced Settings to open the Windows Firewall with Advanced Security dialog box.**
4. **To create a new rule that controls traffic allowed to enter the system, choose Inbound Rules.**
5. **Right-click Inbound Rules and then choose New Rule.**

6. To create a rule that opens a port on the firewall, choose Port and then choose Next.
7. Select the protocol — either TCP or UDP — and then type the port number you want to open and choose Next.

In my example, I am going to create a custom rule to open a port for my web server so I am using TCP and port 80 (see [Figure 2-17](#)).
8. Choose whether you are allowing this traffic through the firewall or blocking it and then choose Next.

I am choosing Allow the Connection.
9. Choose Next to accept the default network locations the rule applies to.
10. Give the rule a name such as “A+ Web Server Port” and then choose Finish.

The screenshot shows the 'New Inbound Rule Wizard' window with the title bar 'New Inbound Rule Wizard' and a close button. The window is divided into a left sidebar and a main content area. The sidebar, titled 'Steps:', contains five items: 'Rule Type' (green dot), 'Protocol and Ports' (green dot and highlighted), 'Action' (blue dot), 'Profile' (blue dot), and 'Name' (blue dot). The main content area is titled 'Protocol and Ports' and has the instruction 'Specify the protocols and ports to which this rule applies.' It contains two sections of radio buttons. The first section, 'Does this rule apply to TCP or UDP?', has 'TCP' selected. The second section, 'Does this rule apply to all local ports or specific local ports?', has 'Specific local ports:' selected, with a text box containing '80' and an example 'Example: 80, 443, 5000-5010' below it. At the bottom right are three buttons: '< Back', 'Next >', and 'Cancel'.

New Inbound Rule Wizard

**Protocol and Ports**  
Specify the protocols and ports to which this rule applies.

**Steps:**

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Does this rule apply to TCP or UDP?

☒ TCP  
☐ UDP

Does this rule apply to all local ports or specific local ports?

☐ All local ports  
☒ Specific local ports:   
Example: 80, 443, 5000-5010

< Back   Next >   Cancel

**FIGURE 2-17:** Windows Firewall with Advanced Security.

Once you have added the rule, you can then enable or disable the rule at any time by right-clicking the rule and choosing Enable Rule or Disable Rule.



**REMEMBER** TCP is used for traffic that requires a connection to be established, and UDP is for connectionless. I want to go with TCP because FTP uses the TCP protocol.

## *Security Center versus Action Center*

The Action Center in Windows is a central window that informs you of critical security mistakes with your system. In the Action Center, you can see whether you have a firewall enabled on your system and whether antivirus software is installed. (If Windows does not see antivirus software installed on the system, it reports virus protection as not found!) You can also see from the Action Center if Windows Update is not receiving automatic updates or if Windows Defender is out of date. Windows Defender is the malware protection software built into Windows.

From the Action Center, buttons are available so that you can manage Windows Defender updates, change your Windows update settings, or even perform a backup.

In the Action Center, you can also change your UAC settings, perform a backup, or perform a restore of a restore point. To get to the Action Center, choose Start ⇒ Control Panel ⇒ System and Security ⇒ Action Center.

## *Implementing Security Best Practices*

In the following sections, you discover some basic best practices that can help you secure your environment. These sections are designed to be a summary of features that I discuss throughout the chapters of this book.

## *Hardening a system*

The first thing you can do to secure your system is to *harden* it: You remove any software that you are not using and disable any Windows services that are not needed. The concept of hardening comes from the fact that hackers compromise systems by leveraging software that is installed or running on the system. The less software you have running, the less likely you are to be hacked!

## *Patching systems*

Regularly patching the system by running Windows Update is critical. As Microsoft finds out about security problems with its OS and software, its programmers fix the problem and deliver the fix through the Windows Update site. To ensure that you are getting the security fixes and patches, you must run Windows Update often. More on this topic in the next chapter.



**TIP**

Even though the feature is called Windows Update, you can get updates for more than just the Windows operating system. You can download updates for a number of Microsoft products from the Windows Update site, such as Windows and Microsoft Office.

## *Firewalls*

Make sure you turn on the Firewall feature in Windows. The firewall helps protect your system from network attacks, but it is not the be-all and end-all of network security. You also need to follow the other best practices presented in this chapter.

## *Password policies*

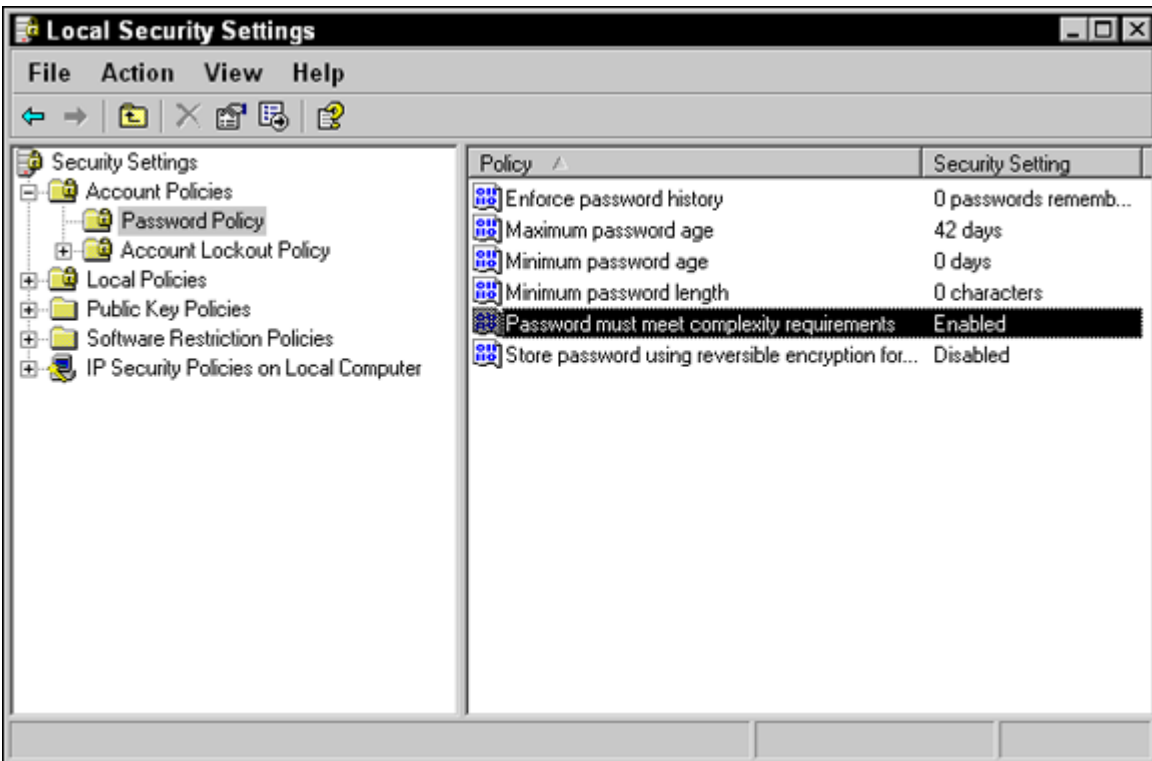
Stress to your users the importance of using strong passwords. To enforce strong password usage, you can set a password policy in the Local



Security Policies. To set the password policy, follow these steps:

1. **In Windows 7, choose Start ⇒ Control Panel. In Windows 8.1, right-click the Start icon and choose Control Panel. In Windows 10, click the Start button and type control, then choose Control Panel from the menu.**
2. **In the Control Panel, click System and Security and then click Administrative Tools, located toward the bottom of the window.**
3. **In the Administrative Tools, double-click Local Security Policy to start the Local Security Policy console.**
4. **Expand Account Policies and highlight Password Policy.**
5. **Ensure that users use strong passwords by double-clicking the Password Must Meet Complexity Requirements policy and then choose Enable (see [Figure 2-18](#)).**

This setting ensures that users use passwords of a minimum of six characters, with a mix of uppercase and lowercase characters, numbers, and symbols. The password will also not contain any part of the username.



**FIGURE 2-18:** Configuring password complexity in Windows.

## ***Auditing***

Make sure that you enable auditing on critical systems so that you will know (hopefully) when the system has been compromised. For example, if a hacker makes his way into the system and builds himself a hidden user account, you will know about it if you have enabled account management auditing.

## ***Encrypt sensitive data***

Another big part of security is ensuring the confidentiality of your data. The best way to ensure confidentiality is to use encryption technologies to encrypt your data as it sits on the hard drive. This ensures that if someone steals your computer or hard drive, he or she will not be able to read the data as it is encrypted.

Windows has a number of features to encrypt data, such as EFS, Bitlocker, and Bitlocker-To-Go.

### ***EFS***

Encrypting File System (EFS) is an older NTFS feature that is designed to encrypt files (and not the entire disk). To encrypt a file with EFS, follow these steps:

- 1. Right-click the file you want to encrypt and then choose Properties.**
- 2. On the General tab, choose the Advanced button at the bottom of the screen to go to the Advanced Attributes dialog box.**
- 3. Select the Encrypt Contents to Secure Data check box and then choose OK twice to exit out.**

Keep in mind that this is a feature that is designed to be transparent to the users. Once the file is encrypted, as soon as you open the file it is automatically decrypted. When you close the file, it is again encrypted to disk.

Once you have encrypted the file you can go back to the Advanced Attributes dialog and add additional people who can decrypt the file. Underneath the scenes EFS uses certificates to encrypt the information.

### ***BitLocker***

BitLocker is a Windows feature that allows you to encrypt the entire disk. This ensures that if someone steals your hard drive and then tries to connect it to another system to read the data, he or she will be unsuccessful because the entire drive is encrypted. Keep in mind that BitLocker is only available to the Ultimate and Enterprise editions of Windows Vista and Windows 7, and the Pro and Enterprise editions of Windows 8.1.

With BitLocker you can have the encryption keys stored in a computer chip on the computer, known as a Trusted Platform Module (TPM). A TPM is a chip on the motherboard that is used to store encryption keys that can be used by BitLocker to encrypt the drive. You can also use BitLocker in USB key mode where the keys are stored on a USB device. This means you would need the USB key to be able to decrypt and access the drive.

## ***BitLocker-To-Go***

BitLocker-To-Go is the Windows feature that allows you to encrypt the contents of a removable drive such as a USB drive. This ensures that if your USB drive that contains sensitive data is ever lost, you have the confidence of knowing the data is unreadable on the drive.

## ***Use switches instead of hubs***

You can enable a number of security features when working with switches instead of hubs on the network. To begin with, switches filter traffic by sending only data to the port on the switch that the data is destined for. This can add to the security of the network because it is harder for a hacker to monitor network traffic when the port the hacker is using is not getting a copy of all data — just data destined for his system.

The second thing you could do to secure your environment with a switch is disable any unused ports on the switch. This way, if the hacker gets physical access to your network, she cannot simply plug into the switch to get access to the network.

The other thing you could do with more advanced switches is to configure a *virtual local area network* (VLAN), which is a grouping of ports on the switch that are allowed to communicate with one another but cannot communicate with other VLANs on the same switch. For example, I have a 24-port switch with two VLANs. The first VLAN comprises the first 12 ports, and the second VLAN comprises the last 12 ports. Any systems plugged into the first 12 ports cannot communicate with the systems on the second set of 12 ports, and vice versa. Essentially, you have two networks — but only one switch.

## ***Use antivirus software***

Using antivirus software is another security best practice. Ensure you are using antivirus software on all your systems and keep the virus definition database up to date! Antivirus software is designed to protect your system against viruses. For more information on antivirus software, check out Book 9, [Chapter 3](#).

## ***Securing wireless***

As a last note, I just want to add a few tips here to help secure your wireless environment. You can configure most of these settings on the wireless router by navigating to the administration site of the router, which involves starting a web browser and entering either 192.168.0.1 or 192.168.1.1. If you have hit the web administration pages of the wireless router, you will be asked to log on. Most routers have a default username of admin with no password that you will use to logon.

After you are logged onto the router, locate the following options in the administration pages:

- » **Router password:** After you hook up your wireless router, be sure to connect to the router and change the admin password. Most wireless routers ship with no password, so be sure to protect your router by assigning one. Check the documentation that came with your router to find out how to set an admin password.
- » **Setting the SSID:** The *Service Set Identifier (SSID)* is a name assigned to your wireless network. You should change the name of the SSID, but do not use your company name. When hackers are “*war driving*,” they pick up on a signal from a wireless network. Say the SSID says “BridgetsWidgets.” Hackers then look for the building with the Bridget’s Widgets sign. When they spot the sign, they then drive close to the building so that they get a stronger signal. Don’t make it easy for them to figure out what building to get close to!
- » **Disabling SSID broadcasting:** After you set the SSID, you also want to disable SSID broadcasting. The wireless router broadcasts the SSID so that anyone who gets close will know the wireless network is there. If you disable broadcasting, then to connect to the wireless network, a person has to know and input the SSID manually into his network client. Keep in mind that programs such as Kismet can still discover a wireless network that has SSID broadcasting disabled.
- » **MAC address filtering:** If you check the administration pages on your wireless router, there is a place for you to enable MAC address filtering. This feature allows you to control which systems can connect to the wireless network by the MAC address of their network

card. After MAC address filtering is enabled, only the MAC addresses listed can connect to the network. Keep in mind hackers can spoof their MAC address to bypass your MAC filtering so the feature can be compromised if someone is determined.

- » **Enable Encryption (WEP/WPA/WPA2):** Be sure to enable some form of encryption for your wireless network. You can use a number of protocols to encrypt traffic on your wireless network: WEP, WPA, or WPA2, depending upon what is supported by your wireless router. It is important to note that the WEP protocol is easy to crack and should be avoided if possible. Use WPA2 as your wireless encryption protocol when possible.

For more information on wireless networking, check out Book 8, [Chapter 2](#).

## *Getting an A+*

This chapter introduces you to a number of best practices for securing your Windows environment. Some of the key points to remember for the A+ exams are to

- » Create user accounts for each user of the system. Make sure that users use strong passwords for those accounts and understand to not share those passwords.
- » Assign permissions to resources such as folders and files to ensure that unauthorized users don't get access to the resource.
- » Enable auditing so that you are aware of any security-related events that happen on the system. Also be sure to review the security log often.
- » Enable a firewall for the network and enable the Firewall on the Windows system.
- » Secure your wireless router by disabling the wireless feature if you are not using the wireless components of the router. If you are using

wireless, be sure to implement WPA2, MAC filtering, and disable SSID broadcasting.

## *Prep Test*

**1. You are the IT technician for a company and working on ways to secure the system. You would like to control network traffic that enters into the Windows 8.1 system. What security feature stops network packets from entering the system through the network card?**

- (A) Auditing
- (B) Password policy
- (C) Permissions
- (D) Firewall

**2. What is the network name assigned to the wireless network?**

- (A) WEP
- (B) SSID
- (C) SID
- (D) WPE

**3. You are securing a folder and want to allow a user to read, modify, create, and delete a file. What permission would you assign?**

- (A) Read
- (B) Full Control
- (C) Modify
- (D) Deny

**4. You are working with the security team within your company to ensure systems are configured securely and monitored on a regular basis. You have enabled auditing; where do you go to view the audit information?**

- (A) Local Security Policy
- (B) Event Viewer
- (C) LAN Connection Properties
- (D) Firewall

**5. A privilege to perform an operating system task is known as what?**

- (A) Permission
- (B) Policy
- (C) Right
- (D) Firewall

**6. You need to give Sue the capabilities to manage permissions on a file. What permission allows her to modify the permissions?**

- (A) Read
- (B) Full Control
- (C) Modify
- (D) Deny

**7. Management has requested that users be able to change the time on the computer. What is the best way to allow Bob to change the time on his computer?**

- (A) Enable an Audit Policy.
- (B) Place Bob in the Administrators group.
- (C) Assign Bob the Change System Time permission.
- (D) Assign Bob the Change System Time right.

**8. Which security features might you enable through the system BIOS?**

- (A) Boot devices
- (B) Password policy
- (C) Permissions



(D) Audit policy

## *Answers*

1. **D.** A firewall is designed to stop data from entering your system through the network card. See “[Implementing Firewalls](#). ”
2. **B.** The SSID is the name assigned to the wireless network. Review “[Securing wireless](#). ”
3. **C.** To allow users to read, modify, create, and delete a file, you assign the Modify permission. Check out “[Implementing Permissions and Rights](#). ”
4. **B.** When auditing has been enabled, you view the auditing information by reviewing the security log in Event Viewer. Peruse “[Implementing Auditing](#). ”
5. **C.** A right gives you the privilege to perform an operating system task. Take a look at “[User rights](#). ”
6. **B.** The Full Control permission allows users to modify permissions on a file or folder. Peek at “[Permissions](#). ”
7. **D.** You would assign Bob the Change System Time right. You could put Bob in the Administrators group, but that is not the best answer because you have given him a number of other capabilities at the same time. Look over “[User rights](#). ”
8. **A.** The boot devices can be disabled through the BIOS, which controls whether someone can bypass your operating system by booting from a bootable CD or floppy. Study “[Securing Systems through BIOS/UEFI](#). ”

# Chapter 3

## Viruses and Malicious Software

---

### IN THIS CHAPTER

- » Understanding viruses
  - » Looking at malicious software
  - » Performing software updates
  - » Recovering an infected system
- 

In this chapter, you find out about the different types of malicious software that you might encounter after you connect your system to the Internet or start sharing files with another system. As a service technician, you will spend most of your time trying to fix a computer that is polluted with viruses or other forms of malicious software.

Being able to protect your system from viruses and other forms of malicious software is an important skill to have. You also have to know how to perform a virus scan and remove viruses from your system.

## *My Computer Has a Virus!*

A *virus* is a piece of software designed to do harm to the system in one fashion or another. The virus is typically associated with a host file, such as a word processing file or video clip; and when that file is opened, the virus is activated and does its damage to the system. The damage could be disastrous in the sense that the system no longer starts up, or it might just create a faulty system that is annoying to work with. Either way, the virus has done its job — to cause pain and suffering in your computer's life, and yours!

### *Types of viruses*

A number of different types of viruses can infect your system:

- » **Boot sector:** A *boot sector* virus attacks the boot code contained in the boot sector of the disk. This type of virus loads every time the system boots up and sometimes may even prevent the system from booting.
- » **File:** A *file* virus attaches itself to an executable file and is run, or activated, when the executable file is run. This has been one of the most popular forms of viruses for many years because the attacker simply has to trick you into running the executable.
- » **Macro:** A popular type of virus today is the *macro* virus. A few years ago, Microsoft was promoting the fact that you could program your own macros to customize Microsoft Office applications (such as Word, Excel, and Access). A *macro* is a set of Visual Basic for Applications (VBA) commands that performs a specific task. VBA can also be used to call other programs. For example, I created a macro in Excel that automatically starts Outlook and emails the contents of the spreadsheet to one of my business partners.

My point is that VBA is pretty much a full programming language. And the fact that VBA is a programming language is important because it can perform a lot of powerful actions, such as creating, deleting, and modifying files. Fear not, though. The following section explains how to keep yourself safe with the Office macro security settings.

You might also encounter worm viruses or Trojan viruses, but I save those for discussion in “[Understanding Malicious Software](#),” later in this chapter.

## *Office macro security settings*

After the power of VBA became known, hackers started creating malicious macros in Word and Excel documents so that when you opened the documents, the macro would run and cause damage to your system. To prevent this from occurring, you could change the macro security settings in each Office application to control how to manage macros found in documents when the document is opened.

» **Office 2003:** To change the macro security settings in these versions of Office, choose Tools ⇒ Macro ⇒ Security in your Microsoft Office program and then choose one of the following options (shown in [Figure 3-1](#)):

- *High:* Only macros from trusted sources are allowed to run; all other macros are disabled. This is the highest level of security because most macro code is not created from trusted sources.
- *Medium:* Office prompts you to decide whether to enable or disable macro support every time you open the file. This is a good setting because if you were unaware that a file had a macro, you could choose to disable macros while the file is open — knowing that if there is malicious code in the file, it won't run.
- *Low:* All macros run without your knowledge. If you have no worries about macro security, you may set this option — but never open a Microsoft Office document unless you know where it came from!

» **Office 2016:** Choose File ⇒ Options ⇒ Trust Center, then choose the Trust Center Settings button. From the Trust Center window that opens, select one of the following radio buttons:

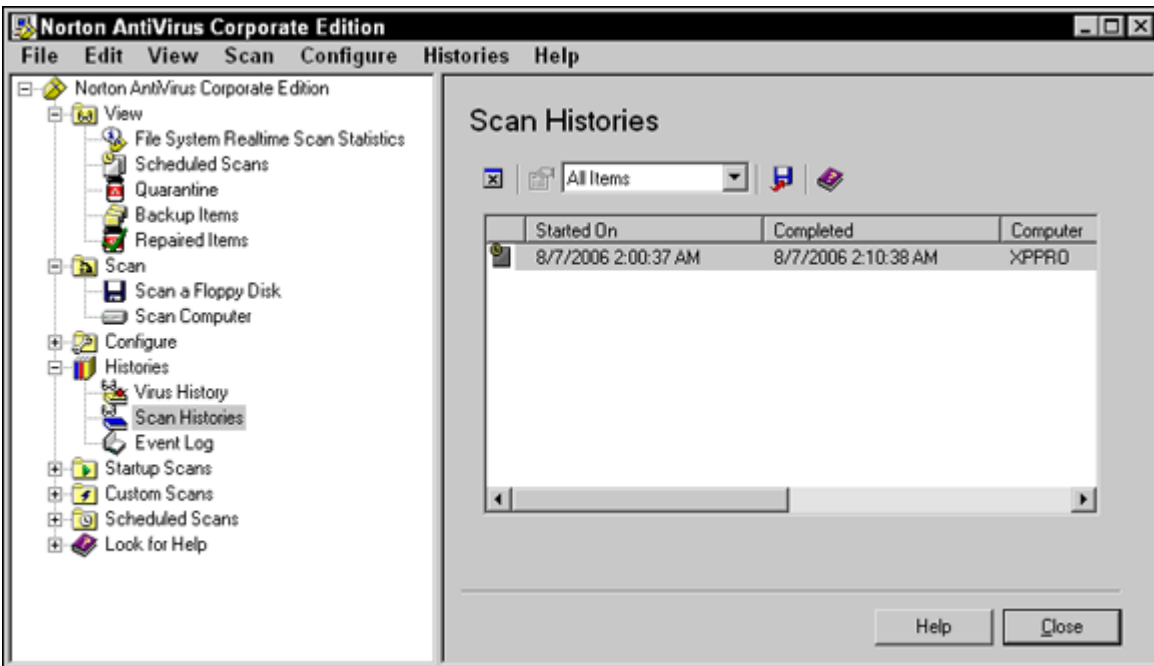
- *Disable All Macros without Notification:* Macros are disabled but you are not notified.
- *Disable All Macros with Notification:* Notifies you that macros have been disabled.
- *Disable All Macros Except Digitally Signed:* Signed code is code that is considered safe to run on your system. Choosing this option will only run macro code that has been signed.
- *Enable All Macros (Not Recommended):* Allows unsigned and signed macros to run. This is not recommended as potentially dangerous code could execute and negatively change your system.



**FIGURE 3-1:** Configuring macros security settings in Microsoft Office.

## *Protection from viruses*

To protect your computers and servers from viruses, it is essential that you have virus protection software installed. Simply, such software, such as the program shown in [Figure 3-2](#), knows about the different viruses and can either remove the virus or remove files from your system that contain viruses.



**FIGURE 3-2:** Looking at virus protection software.

You can choose from many different name brands of virus-protection software, each of which has its own benefits. Some of the popular names in virus protection are

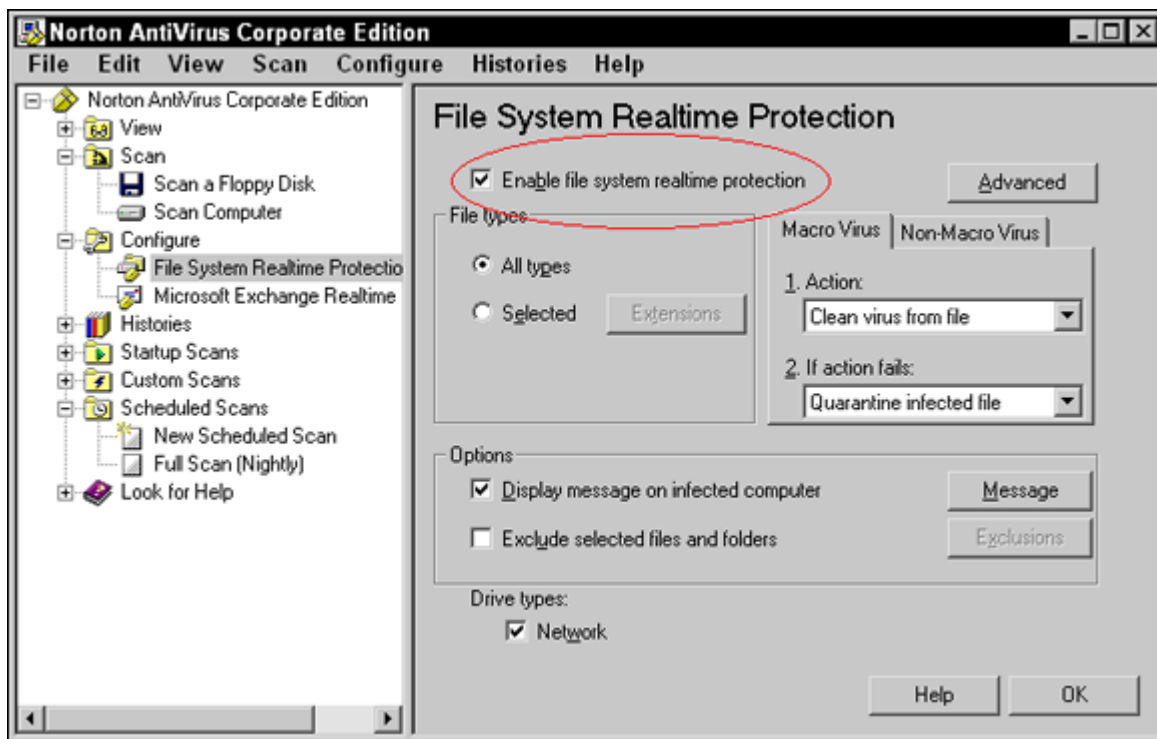
- » **McAfee:** [www.mcafee.com](http://www.mcafee.com)
- » **Norton/Symantec:** [www.symantec.com/norton/index.jsp](http://www.symantec.com/norton/index.jsp);  
[www.symantec.com/index.jsp](http://www.symantec.com/index.jsp)
- » **Panda Security:** [www.pandasecurity.com](http://www.pandasecurity.com)
- » **F-PROT:** [www.f-prot.com](http://www.f-prot.com)

Each antivirus software product has its own benefits and features. For example, you might prefer the interface or usability of one product over another. Still, each product should offer similar features. When shopping for antivirus software, you should look for software that offers at least the following features:

- » **Scheduled virus scans:** This is a great feature because you can have the virus scanning software scan the system in the middle of the night (when the system is not being used), and you do not have to physically

perform the scan yourself. You may also choose what happens when a virus is found: say, attempt to remove the virus from the file, place the file in a quarantine area, or delete the file.

- » **Real-time protection:** The virus protection software runs in memory all the time and scans any file that you open. The benefit of real-time protection is that you are protected from viruses between scan times. Be sure to have software that supports real-time protection and have the feature enabled (see [Figure 3-3](#))!
- » **Scheduled definition updates:** Virus definitions are what virus protection software uses to update its knowledge of viruses. Your virus protection software should have a feature that allows the definitions to be downloaded from its vendor site.
- » **Scanning email:** Many virus protection software versions support scanning email messages as they arrive in your inbox. This is typical of virus protection software that runs on an email server and you usually pay an annual subscription fee for the service.



**FIGURE 3-3:** Enable real-time protection within antivirus software.

Note that today we have antivirus software and anti-malware software. Antivirus software would protect you against viruses, while anti-malware software protects you against many different forms of malicious software such as viruses, spam, spyware, and adware. An example of anti-malware is Windows Defender.

## *Updating virus definitions*

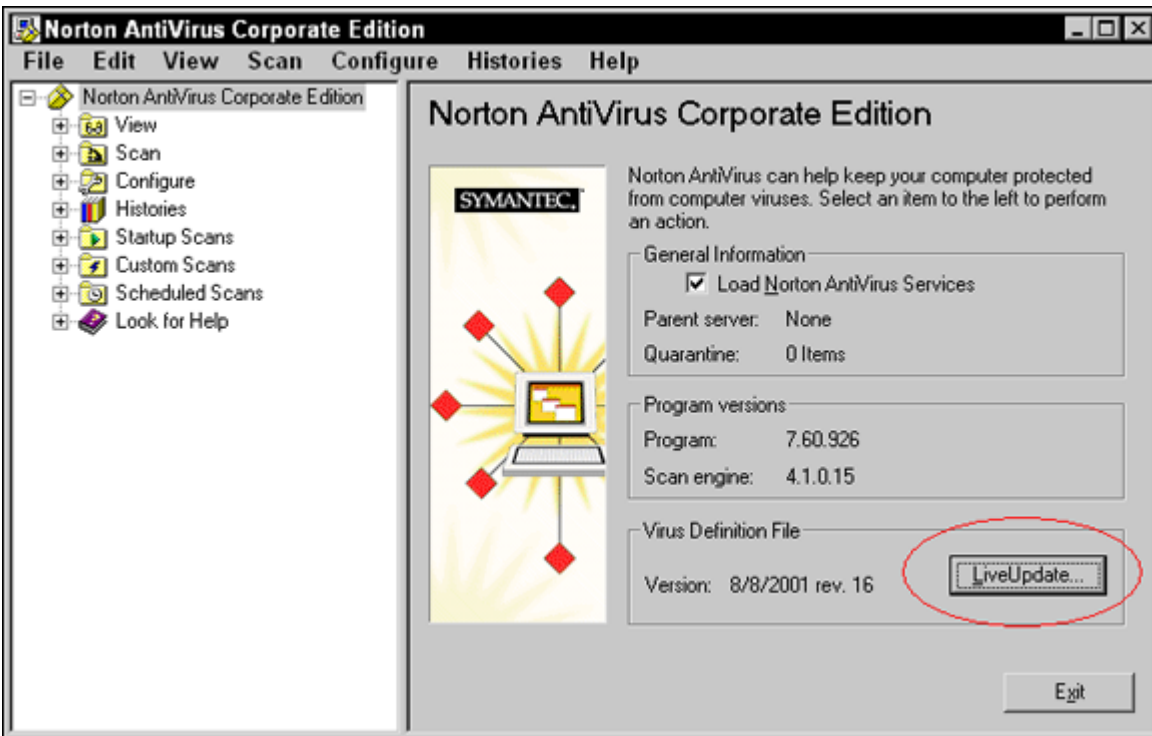
When you perform a virus scan, your virus protection software knows only about the viruses as of the creation time of the software. This is a huge problem because new viruses appear every day.

So, to keep your software valid and to allow it to still be useful years after you purchase it, manufacturers use virus definitions as a way for the software to know the current list of viruses. The virus definitions can be updated online. So, even though your software might be two years old, you can keep it current.

It is critical that you update your virus definitions regularly, or your virus protection software won't know about any new viruses that are developed.

To update the virus definitions in my Norton Security (formerly Norton Antivirus), after I start the software, I see a LiveUpdate button on the main screen, as shown in [Figure 3-4](#). To update my virus definitions, I simply click the LiveUpdate button; updating virus definitions should be this simple in most other antivirus programs as well. It is also important to notice that the antivirus software displays how up to date the virus definitions are.





**FIGURE 3-4:** Updating virus definitions within antivirus software.

## *Understanding Malicious Software*

Other types of malicious software, outside of your typical viruses, attack systems every day. The following sections outline other types of malicious software — but understand that they are all considered types of viruses.

### *Trojan horses*

*Trojan horses* are special programs that do something totally different than what the user who runs it thinks it does. For example, NetBus is a very popular Trojan virus that ships as a file called `patch.exe`. A hacker emails the file called `patch.exe` and explains in the email that this is a security patch you need to apply to make sure your system is secure. Unfortunately, `patch.exe` is the security hole! When you run `patch.exe`, it opens your system up to the hacker by opening a port so that the hacker can connect to the port at any time and control your system.

Trojan viruses are normally loaded on your system by the hacker tricking you into running the program on the system, typically through an email

message. You can remove the Trojan with virus protection software.

## ***Worms***

A *worm* is a self-replicating virus: The worm doesn't need to be activated by the user opening the file. Rather, a worm is a virus that runs on a system and also tries to infect other systems on the network. Worm viruses can be replicated to other systems on the network automatically, or they could replicate to a flash drive when you insert a flash drive into an infected system. Then when you take the flash drive to another computer, the worm automatically transfers from the flash drive to the other system.

Worms are loaded on your system by connecting to your system across the Internet. The worm is usually designed to infect the system by connecting through a specific piece of software. For example, the Nimda worm virus was designed to infect any system running Microsoft Web Server software (Internet Information Services [IIS]) and would replicate across the Internet infecting IIS web servers.

To prevent a worm from infecting your system, be sure to have a firewall and make sure that you are up to date with patches. For more information on firewalls, check out Book 9, [Chapter 2](#). For more about staying up to date, read the “[Preventing Problems by Staying Up to Date](#)” section in this chapter. To remove a worm from your system, you can try your antivirus software, or you may have to download a removal tool specific for that worm. For example, Microsoft offers a malicious code removal tool that you can download from [www.microsoft.com/downloads](http://www.microsoft.com/downloads).

## ***Spyware and adware***

*Spyware* is software that loads on your system and then monitors your Internet activity. *Adware* is software that creates pop-ups from time to time advertising a particular product or service.

Both types of viruses infect your system when you surf the wrong Internet site. Spyware and adware have become a huge negative result of the Internet, so a number of products are available to eliminate spyware and adware. The most popular products used to eliminate spyware and adware are

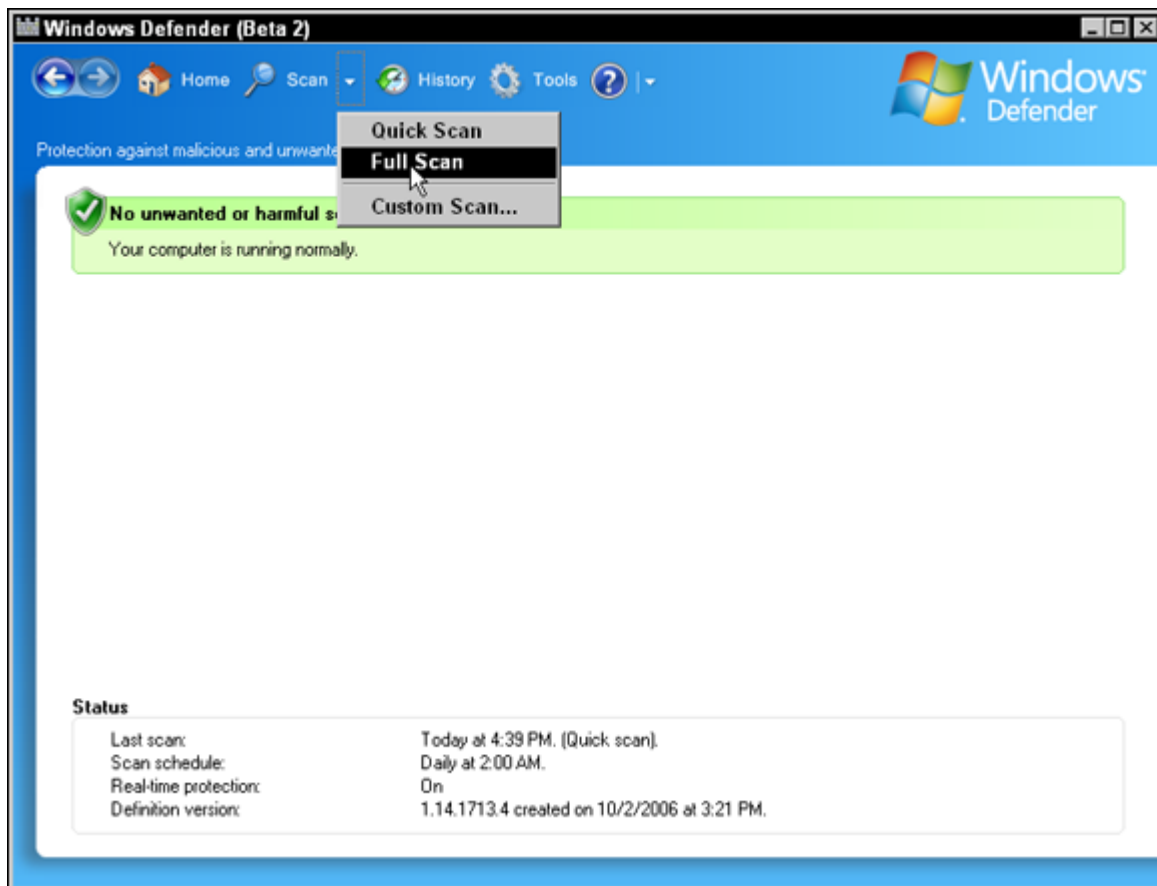
» **Spybot Search & Destroy:** [www.safer-networking.org/en/download](http://www.safer-networking.org/en/download)

» **Ad-Aware:** [www.lavasoft.com](http://www.lavasoft.com)

» **Microsoft Windows Defender:**

[www.microsoft.com/windows/products/winfamily/defender/default.aspx](http://www.microsoft.com/windows/products/winfamily/defender/default.aspx)

Windows Defender originally was a free download from Microsoft's website, but was later incorporated into later versions of Windows such as Windows 7, Windows 8.1, and Windows 10. (See [Figure 3-5](#).)



**FIGURE 3-5:** Remove spyware with Windows Defender.

When selecting which software to use for spyware or adware removal, be sure to go with a product that supports features similar to good antivirus software, such as real-time protection and scheduled spyware scans.

## ***Ransomware***

*Ransomware* is a type of malicious software that takes control of a system usually by encrypting the contents of the drive so that you cannot access the system. After the malicious code encrypts the drive, the user is notified that the system has been locked and that to unlock it, the user usually needs to pay a certain amount of money.

## ***Other malicious software***

There are a number of other types of malicious software you may encounter in the real world and on the A+ certification exams. Be sure to be familiar with the following types of malicious software:

- » **Keylogger:** A keylogger can be software on the system that records all your keystrokes to a file and then sends that file to the hacker via email at a later time. Keyloggers can also be a hardware device connected between your keyboard and the computer that stores all your keystrokes to be reviewed at a later time by the hacker.
- » **Rootkit:** A rootkit is malicious software hidden on the system that is designed to give the hacker administrative access to the system, known as “root-level access” in some operating systems.
- » **Botnet:** A botnet is a group of systems that the hacker has already hacked into and is controlling. These systems under the control of the hacker are then all used to perform a bigger attack on another victim. For example, a hacker may use a botnet to perform a denial of service attack against a website.

## ***Pop-ups and phishing***

To help protect your system from malicious activity when surfing the Internet, browsers such as Chrome, Firefox, Safari, and Internet Explorer (IE) have built-in pop-up blockers and prevent phishing attacks. Windows has these features enabled by default, protecting you from malicious content on the web!

A pop-up blocker prevents additional windows from launching when you are surfing a website. Websites and adware often have pop-ups appear to

promote products. With a pop-up blocker enabled, though, you are notified by a yellow bar at the top of the browser indicating when a pop-up is blocked. Click the yellow bar to allow the pop-up.

Windows OSes running newer versions of IE (IE 7 or greater) have built-in phishing protection features, known as Phishing Filter, that allows you to check the authenticity of a website to ensure that it is not a known “phishing” site. If the site is a known phishing site, the browser will block the site. For more information about phishing, see Book 9, [Chapter 1](#).

## *Identifying Hoaxes*

It is important to understand that some malicious code that you hear about is a *hoax*! For example, I remember a few years back, I was playing an elf bowling program that everyone was emailing around at Christmastime. After weeks of playing this game, it was said that the program should be removed from your system because on a certain date it would do damage to your system. I removed the program from my main computer, but I ran the program on a test system after that date, and it did no harm.

You typically receive hoaxes about viruses through your email system. The email you receive is acting as a virus alert, but unfortunately, there is no actual virus to report — it is a hoax. The benefit of such hoaxes is for the creators of the *actual* viruses; hackers hope that you receive so many hoaxes that you eventually ignore true virus alerts.

If you receive an email or other form of notice about a virus, check it against a virus hoax list to see whether the warning message is a hoax or has merit. Most virus protection software manufacturers keep an up-to-date list. You can go to a generic hoax site like Hoaxbusters, which is found at [www.hoaxbusters.org](http://www.hoaxbusters.org).

## *Preventing Problems by Staying Up to Date*

One of the most popular techniques hackers use to compromise systems is to find vulnerabilities in the software you use day in and day out. For example, hackers quickly figured out a way to perform the “dot dot” attack on Windows 2000 systems after IIS was installed. With the “dot dot” attack, hackers navigate the folder structure of a web server and delete files — a serious security flaw. After Microsoft got wind of the mistake, its programmers created a fix. It is your responsibility as a network administrator to download all the fixes to problems in the software you use.

## *Windows Update*

To make it easier for you to get security fixes (patches) and updates for Microsoft software, use the Windows Update feature within the operating system. If you choose the Windows Update command from the Start menu, you are automatically connected to the Microsoft Windows Update site, where your system is scanned for which updates are needed.

Windows Update allows you to do an express update where all critical updates are installed on your system, or a custom update where you get to select which updates to install. From the Windows Update site, you install all the updates or patches that your system needs. Performing a Windows Update is a critical step to securing your systems — be sure to do it regularly. You can access Windows Update in Windows 7 and Windows 8 from the Control Panel using these steps: Navigate to the Control Panel and then choose System Security ⇒ Windows Update. From the Windows Update screen, click the Check for Updates button to manually check for updates.

Microsoft has started using the term Microsoft Update instead of Windows Update because you can now update all the Microsoft software, not just the Windows operating system.

## *SUS and WSUS*

Most companies have thousands of systems on the network, which would make it impossible to visit each system individually and run Windows Update. To solve the problem of deploying updates to thousands of systems at a time, Microsoft created Windows Server Update Services

(WSUS). The WSUS software is loaded on a server and gets all the updates from the Windows Update site. After the WSUS server downloads all the updates, you review and approve the updates. The Software Update Service (SUS) software then sends the updates to the other systems on your network. This means that you don't have to run Windows Update on every system on your network — saving you time and money! This also gives you the added benefit of saving on bandwidth used because the clients get their updates from the WSUS server and not the Internet.

The software update service was improved a few years later to create Windows Server Update Services (WSUS). WSUS solves a number of problems that existed in the original SUS feature that Microsoft had a few years prior. Some of the benefits of WSUS over the older SUS are:

- » **Synchronization:** In this context, *synchronizing* involves downloading updates from the Microsoft Update site to the SUS server. When you synchronize the SUS server with Windows Update, it takes hours because all the updates on the Windows Update site are downloaded to your SUS server. This makes no sense because you receive updates for software you don't use, thus wasting time and space on your system. WSUS downloads a listing of updates when you choose to synchronize the WSUS server. After you get the listing of updates, you then select which updates to download — saving space and time!
- » **Product selection:** With WSUS, you can select which Microsoft products you use so that you get a listing of updates for only those products. For example, if you aren't using Microsoft Exchange server, it doesn't make sense to get updates for that product. With WSUS, you can specify that you are not using that software, and the updates for that software do not appear in the list.
- » **Computer groups:** With WSUS, you can deploy updates to selected groups of systems. This is a big improvement over SUS because with SUS, when you approve the update, the update gets sent to all the systems. With WSUS, you can create groups of computers, and when you approve an update, you assign it to a group. For example, you

could create a group called Accounting and then place all the accounting computers in that grouping, which allows you to approve updates for just the accounting systems if you like.

## *Antivirus*

A big part of keeping your system up to date is making sure that you download security fixes from the Windows Update site or from the WSUS server, but you also need to be sure that you update the virus definitions for your virus protection software. You want to make sure that you investigate how to update the virus definitions with your antivirus software. The virus protection software should also give you the opportunity to schedule virus definition updates.

## *Other security software*

In addition to virus protection software and Windows Update, you should be aware of a number of other software products.

Microsoft has malicious software removal utilities called the Malicious Software Removal Tool (MSRT) that you can download from [www.microsoft.com/downloads](http://www.microsoft.com/downloads). The MSRT is updated the second Tuesday of every month and is designed to remove the most recent list of viruses from a system. This is a great utility to use when trying to clean an infected system. It is important to note that this is virus removal software — not virus protection software. You should always run your virus protection software, but if you need to remove a virus from an infected system you can use the Malicious Software Removal Tool!

One of the most beneficial types of software out there for network administrators is *vulnerability assessment software*, which can scan all the systems on your network and alert you to any missing security patches or whether you are breaking any major security best practices, like not having a password on your administrator account. The Microsoft vulnerability scanner is Microsoft Baseline Security Analyzer (MBSA) (shown in [Figure 3-6](#)), which you can download from [www.microsoft.com/downloads](http://www.microsoft.com/downloads).





**FIGURE 3-6:** MBSA identifies any security issues with your system.

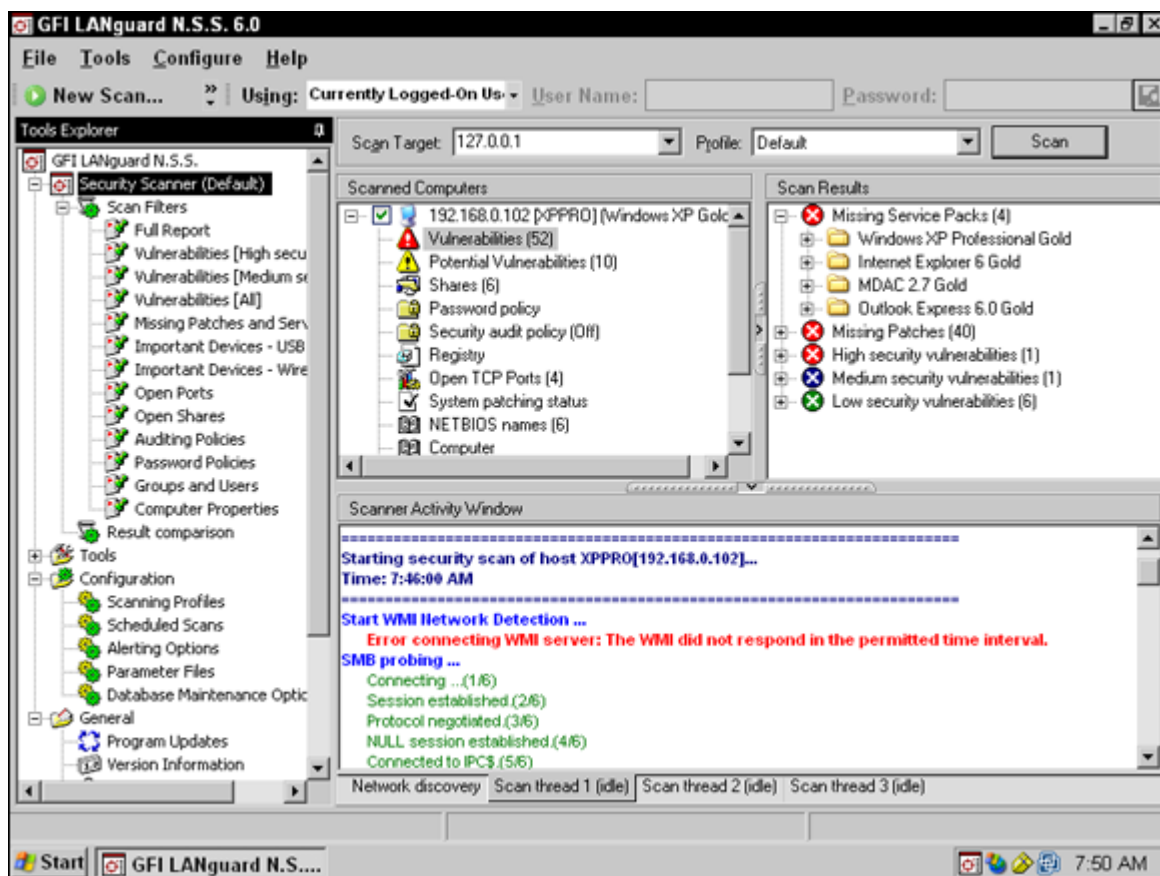
The MBSA identifies a number of issues surrounding the security of your system. A few examples of the types of information you will be presented with are

- » **Windows vulnerability checks:** MBSA verifies that your current system is up to date with operating system patches. It also identifies any security best practices that have been broken.
- » **Weak passwords:** MBSA ensures that all the user accounts have strong passwords.
- » **IIS and SQL Server vulnerabilities:** MBSA verifies that any IIS and SQL Server machines you are using are up to date with security patches specific to those products.

Another example of a vulnerability scanner that is a commercial product available for purchase is LANguard network security scanner from GFI

([www.gfi.com/lannetscan](http://www.gfi.com/lannetscan)). LANguard is very similar to MBSA but offers much more detail with regard to the overall picture of the network and how secure the systems are. LANguard (shown in [Figure 3-7](#)) has the benefit of logging the information to a Microsoft Access database or an SQL server so that you can create your own reports on the information collected. LANguard collects vulnerability information and also reports the following information:

- » Information on the password policy
- » Existing groups
- » Existing user accounts
- » Running services
- » Existing shares
- » NetBIOS name information



**FIGURE 3-7:** Use LANguard to identify security issues with a system.

To practice performing a Microsoft Update to your system, check out Lab 3-1. To practice using the Microsoft Baseline Security Analyzer (MBSA), check out Lab 3-2. Lab 3-1 and Lab 3-2 can be downloaded from the companion website at [www.dummies.com/go/aplusaio](http://www.dummies.com/go/aplusaio).

## *Recovering an Infected System*

One of the challenging aspects of system support is knowing how to remove a virus or malicious software from an infected system and return that system to a functioning state. The following sections are designed to help you identify a system that has been infected, list some of the tools you can use to recover the system, and then give you a list of best practices to follow to keep your systems clean of malicious software.

### *Common symptoms of an infected system*

The first step to recovering an infected system is to be able to identify the symptoms of an infected system. The following is a listing of symptoms that indicate your system is infected with malicious software or under attack by a hacker:

- » **Pop-ups:** If you have a lot of windows pop up when trying to surf the Internet, you most likely are infected.
- » **Browser redirection:** If you launch your web browser and are redirected to another site outside of your default home page, you most likely are infected. If you type a website address into the browser and a different website displays, you most likely have been redirected by malicious software running on your system.
- » **Security alerts:** If you get a number of security alerts, you most likely are infected.  
The security alert is often a pop-up created by the malicious software trying to get you to click a link.
- » **Slow performance:** If you notice that your system is insanely slow, the system might be too busy because it is running the malicious software. Also, you may notice that the hard drive is always thrashing

(working hard), which is a good sign that the malicious software is causing disk I/O.

- » **Internet connectivity issues:** If you experience network issues where you are connected, then you are not, then you are connected again, this could be due to malicious software.
- » **PC/OS lockups:** A great sign that your system has been infected with malicious software is when you find that your computer locks up a lot and you have to power the system off and then on again to be able to use it.
- » **Application crash:** Another common sign your system has been infected with malicious software is if you find applications crash a lot. A good example of this is if the web browser crashes on a regular basis.
- » **OS updates failures:** A lot of viruses will prevent you from doing a Windows update. If you find that updates happen very quickly, it is possible they are not happening at all.
- » **Rogue antivirus:** If you find different antivirus software installed on the system or even if you find that your antivirus updates happen very quickly, it is possible that the virus has disabled your antivirus software and/or antivirus updates.
- » **Spam:** If you receive a number of unsolicited emails, this could be due to malicious software. You most likely are receiving the spam because you have given your email address to different websites.
- » **Renamed system files:** If you find that system files are being renamed, this is an indication of a virus. Also, if you find a number of additional folders and files on your system, you may have been hit with a virus.
- » **Disappearing files:** If you find that a number of files are missing from your system for no reason, this could be due to a virus.
- » **File permission changes:** If you cannot explain changes to the system, such as file permissions or even configuration changes, this could be due to a virus.

- » **Hijacked email:** If you have people replying to messages that you did not send, your email could have been hijacked by malicious software. If your email software has been hijacked, you may receive responses from users regarding email messages they received from you, but you did not send to them. You may also experience automated replies from users for an unknown email message that you did not send.
- » **Access denied:** If you find that you are getting access denied messages on folders and files that you should have access to, you may have been hit with a virus.
- » **Invalid certificate (trusted root CA):** When browsing to secure sites you notice the address bar is red and you get a certificate warning that the certificate is untrusted or invalid, this may indicate that your browser has been redirected to an untrusted, unsecure website. This redirection is a great sign that your system has been infected with malicious software.
- » **System/application log errors:** You should be checking log files on a regular basis for any major issues with a system. In the system and application log you may notice suspicious events, such as changes being made to the system that you did not perform. This could be an indication of malicious software making changes on your behalf.

## *Tools used to protect the system*

To protect your system from malicious software, you can use a number of tools. This chapter introduces a number of methods already, but I want to make sure that I summarize them before leaving the chapter. The following tools are useful for protecting your system from malicious software:

- » **Antivirus software:** The most important protection method is to ensure that you have antivirus software installed and that the definitions are up to date. The A+ certification exams are sure to test you on this.
- » **Anti-malware software:** If your antivirus software does not provide other malware protection such as adware protection, you may need to install additional malware protection.

- » **Antispyware software:** Again, if your virus protection software does not protect you from spyware, you will need to install some antispyware protection software.

## *Tools used to remove infection*

In addition to knowing what tools you need to install to help protect against viruses and malware, it is important to know what tools you can use to help remove malware from an infected system. The following tools can help you remove unwanted malware:

- » **System Restore/Snapshot:** The most important feature to use to help remove malicious software is the System Restore feature. Using System Restore, you can revert your system to the way it was a number of days ago. To access System Restore, go to Control Panel ⇒ System. From the System screen choose the System Protection link on the left side. To revert your system to a previous restore point, choose the System Restore button. Walk through the wizard and choose a date to revert your system to. This has saved me hours of work in the past! If you want to create a restore point, choose the Create button at the bottom of the screen.

I have seen cases where System Restore did not work due to the virus preventing it from launching, so in that case, be sure to boot to Safe Mode first (press F8 while booting) and then run System Restore.

You can find out more about System Restore by checking out Book 7, [Chapter 3](#).

- » **Event Viewer:** The Event Viewer can be used to view error messages and status messages on the system and can help you identify problems with the system. Look back to Book 7, [Chapter 1](#) to find out more about Event Viewer.
- » **Terminal:** You could use a terminal, or command prompt, session to remove a virus or fix a system infected with a virus. The value of the terminal or command prompt is that you may find the GUI shell is locked down by the virus, so going to a command prompt is your only choice.

- » **Recovery Console:** The Recovery Console is a command-prompt interface that helps with a number of issues such as a corrupt boot record, corrupt partition table, and disabled services. You can use the Recovery Console to fix problems related to disk errors and missing files. Look back to Book 7, [Chapter 3](#) to find out more about the Recovery Console.
- » **Preinstallation environments:** The Windows PE is a mini-version of Windows that can help you with issues surrounding missing files. Look back to Book 7, [Chapter 3](#) to find out more about Windows PE.
- » **Refresh/restore:** Another common method to get rid of a virus on an infected Windows 8 or above system is to refresh your PC, which installs a new copy of Windows without losing your data such as photos, videos, music, or other personal files. You can also do a full restore (known as Reset), which wipes the system and resets it back to the way it was when you purchased it. If you use the Reset option, you will lose all your files.

To access these options in Windows 8, go to the bottom-right corner of the Taskbar until the charm list appears. From the charm list, choose the Settings charm ⇒ Change PC Settings (at the bottom) ⇒ Update and Recovery ⇒ Recovery. You then see the option for refresh your PC (Refresh) and remove everything (Reset).

- » **Backup/restore:** Today's operating systems have a refresh option for you to easily re-install the operating system. Older operating systems do not have that option, so you may have to resort to a traditional backup and restore method. If you are performing regular backups of the system, you can do a restore of an older backup in order to get rid of the virus. It is important to ensure that your backup does not have the virus! So you might have to go with an older backup than you prefer to ensure that you are grabbing a backup copy that was taken before your system was infected.
- » **End user education:** Ensure you educate your users on safe computing practices. For example, educate users to not click links from unknown sources and not to download programs from unknown sources.

- » **Software firewalls:** Ensure every desktop system and laptop computer have the built-in firewall enabled. If the operating system does not have a firewall built-in, be sure to install one that will prevent hackers from accessing the system from across the network.
- » **DNS configuration:** Check the local hosts file on the computer to ensure that it is not populated with bogus entries from a hacker that has compromised a system. Entries found in the hosts file can lead the user to a hacker site without the user's knowledge.
- » **MSCONFIG/Safe boot:** If you are having trouble running virus scan software or virus removal software because the system is unresponsive, you should boot to Safe Mode and then try a System Restore or Refresh of the system. You can also use the System Configuration Utility (MSCONFIG) to alter the boot options and boot to Safe Mode, or you could even disable software from automatically starting.

### *Best practice for malware removal*

To be efficient with malware protection and removal, you must follow a number of best practices. The following are best practices for malware removal:

- » **Identify and research malware symptoms.** The first step in virus removal is to identify a system that is showing symptoms of an infected system. For example, if you notice that the system is running really slowly and has a number of pop-ups appearing on-screen, this could be an infected system!
- » **Quarantine the infected systems.** After you identify that a system is infected, the first thing you should do is quarantine the system: Disconnect it from the network to prevent the virus from spreading to other systems!
- » **Disable System Restore (in Windows).** When a system is infected with a virus, you may consider disabling System Restore at this point, because the last thing you want is to revert to a restore point that has a virus in it!



- » **Remediate infected systems.** After you have taken the previous steps, you are then ready to clean the infected system using some of the tools mentioned in the previous section, “[Tools used to remove infection](#).” The proper steps you should take to ensure that the malicious software is removed is to first update your anti-malware software. Once the software has been updated, do a scan of the system and remove infections. If you have trouble running the anti-malware software, try booting to Safe Mode, which has minimal software running, or use Windows PE to boot from and then run the anti-malware software.

As a final note on best practices, I want to stress some of the best practices for scanning and removal techniques:

- » **Schedule scans and run updates.** It is critical to ensure that you have scheduled your antivirus definition updates and have scheduled regular scans to run in the middle of the night.
- » **Enable System Restore and create a Restore Point.** Use the System Restore feature to remove a virus from the system! System Restore should be enabled by default, but you can verify that by going to your System Properties dialog box.
- » **Educate the end user.** Educate your end users on how to respond to a virus. Ensure that they know how to contact the response team or maybe do a virus scan.

## *Getting an A+*

This chapter introduces the concepts of viruses and malicious software. Some key points to remember when you take the A+ certification exams are

- » A *virus* is a program that does harm to your system.
- » Popular types of viruses are file, boot sector, and macro viruses.

- » Other types of malicious software are Trojan horse viruses, worms, and spyware.
- » You may use antivirus software to remove viruses from your system and antispyware software to remove spyware from your system.
- » Be sure to update your virus definitions on a regular basis so that your virus protection software can protect your system against the most popular viruses.

## *Prep Test*

- 1. You are trying to fix a computer that is showing symptoms of being infected with a virus. You have run your antivirus software multiple times and it does not seem to be picking up any viruses. What should you do?**
  - (A) Update the antivirus software
  - (B) Update the virus definitions
  - (C) Update Windows
  - (D) Apply a Trojan
  
- 2. What type of malicious software does something totally different than what the user expects?**
  - (A) Virus
  - (B) Virus definitions
  - (C) Worm
  - (D) Trojan virus
  
- 3. One of the sales employees of your company has installed a new piece of software on the system, but the system will no longer boot. What type of virus can prevent the system from booting?**
  - (A) File virus
  - (B) Macro virus
  - (C) Boot sector virus

(D) Trojans

**4. Your manager is concerned about some of the malicious code running in Microsoft Office documents that she has been reading about. What type of virus might occur in a Microsoft Office document?**

(A) File virus

(B) Macro virus

(C) Boot sector virus

(D) Trojans

**5. What type of malicious software monitors your Internet activity?**

(A) Adware

(B) Worm

(C) Spyware

(D) Trojans

**6. You are troubleshooting an infected system and have tried to do a System Restore to a previous day, but the system is unresponsive due to the virus. What should you do?**

(A) Reformat the drive and re-install Windows.

(B) Do a system repair from the Windows installation media.

(C) Boot to Safe Mode and run System Restore.

(D) Perform a Windows Update.

**7. What is the best way to ensure that your system is up to date with security patches?**

(A) Virus protection software

(B) Virus definition update

(C) Spyware

(D) Windows Update

**8. You are the network technician for your company. All employees within the company are running Windows 8.1. One of your users has been hit with a computer virus. What is the best way to clean the system and keep the employee files on the computer?**

- (A) Refresh the PC.
- (B) Re-install from the Windows DVD.
- (C) Reset the PC.
- (D) Format and re-install from Windows DVD.

## *Answers*

1. **B.** Virus definitions need to be up to date to ensure that your virus protection software knows about recent viruses. See “[Updating virus definitions.](#)”
2. **D.** A Trojan virus is a piece of software that does something totally different than what the user expected when he installed the application. Review “[Trojan horses.](#)”
3. **C.** A boot sector virus prevents a system from booting because it corrupts the boot sector. Check out “[Types of viruses.](#)”
4. **B.** A macro virus is created in a programming language like VBA, which exists in the Microsoft Office suite. Peruse “[Types of viruses.](#)”
5. **C.** Spyware is the type of malicious software that monitors Internet activity. Take a look at “[Spyware and adware.](#)”
6. **C.** If the system is unresponsive and you cannot get to the System Restore option, try booting to Safe Mode and then running System Restore. Peek at “[Best practice for malware removal.](#)”
7. **D.** You should perform a Windows Update regularly to download current patches to your system. Look over “[Windows Update.](#)”
8. **A.** Starting with Windows 8, you have a Refresh the PC feature that allows you to quickly re-install Windows without losing your personal files. Study “[Best practice for malware removal.](#)”

# Appendix A

## CompTIA A+ Exam Reference Matrix

.....

You can use this chart to identify which chapters to study in preparation for the CompTIA A+ Certified Professional exams. Because you need to take two exams, it is still best to read this entire volume. There is a great deal of overlap between the Essentials exam and all the other exams.

After reading the entire volume, you can use this chart as part of your review. If you go through the objectives and find any area you don't think you know, you can immediately turn to the appropriate chapter for an in-depth review.

### *2019 Examination Objectives — 220-1001*

<b>Domain/Objective/Description</b>	<b>Book-Chapter</b>
<b>1.0 Mobile Devices</b>	
<b>1.1 Given a scenario, install and configure laptop hardware and components</b>	
Hard drive like SSD versus hybrid versus magnetic disk, and 1.8in versus 2.5in	<a href="#">3-6</a>
Keyboard, Memory, Smart card reader, Optical drive, Wireless card/Bluetooth module, Cellular card, Video card, Mini PCIe, Screen, DC jack, Battery, Touchpad, Plastics/frames, Speaker, System board, CPU	<a href="#">3-6</a>
<b>1.2 Given a scenario, install components within the display of a laptop</b>	
Types like LCD, and OLED	<a href="#">3-6</a>
WiFi antenna connector/placement, Webcam, Microphone, Inverter, Digitizer/touchscreen	<a href="#">3-6</a>
<b>1.3 Given a scenario, use appropriate laptop features</b>	

<b>Domain/Objective/Description</b>	<b>Book-Chapter</b>
Special function keys like Dual displays, Wireless (on/off), Cellular (on/off), Volume settings, Screen brightness, Bluetooth (on/off), Keyboard backlight, Touchpad (on/off), Screen orientation, Media options (fast forward/rewind), GPS (on/off), Airplane mode	<a href="#">3-6</a>
Docking station, Port replicator, Physical laptop lock and cable lock, Rotating/removable screens	<a href="#">3-6</a>
<b>1.4 Compare and contrast characteristics of various types of other mobile devices</b>	
Tablets	<a href="#">3-6</a>
Smartphones	<a href="#">3-6</a>
Wearable technology devices like Smart watches, Fitness monitors, and VR/AR headsets	<a href="#">3-6</a>
E-readers	<a href="#">3-6</a>
GPS	<a href="#">3-6</a>
<b>1.5 Given a scenario, connect and configure accessories and ports of other mobile devices</b>	
Connection types	<a href="#">3-6</a>
Wired like Micro-USB/Mini-USB/USB-C, Lightning, Tethering, Proprietary vendor-specific, and ports (communication/power)	<a href="#">3-6</a>
Wireless like NFC, Bluetooth, IR, and Hotspot	<a href="#">3-6</a>
Accessories like Headsets, Speakers, Game pads, Extra battery packs/battery chargers like Protective covers/waterproofing, Credit card readers, and Memory/MicroSD	<a href="#">3-6</a>
<b>1.6 Given a scenario, configure basic mobile device network connectivity and application support</b>	
Tablets	<a href="#">3-6</a>
Smartphones	<a href="#">3-6</a>
Wearable technology devices like Smart watches, Fitness monitors, and VR/AR headsets	<a href="#">3-6</a>
E-readers	<a href="#">3-6</a>
GPS	

<b>Domain/Objective/Description</b>	<b>Book-Chapter</b>
<b>1.7 Given a scenario, use methods to perform mobile device synchronization</b>	
Synchronization methods like Synchronize to the cloud, Synchronize to the desktop, and Synchronize to the automobile	<a href="#">3-6</a>
Types of data to synchronize like Contacts, Applications, Email, Pictures, Music, Videos, Calendar, Bookmarks, Documents, Location data, Social media data, E-books, and Passwords	<a href="#">3-6</a>
Mutual authentication for multiple services (SSO)	<a href="#">3-6</a>
Software requirements to install the application on the PC	<a href="#">3-6</a>
Connection types to enable synchronization	<a href="#">3-6</a>
<b>2.0 Networking</b>	
<b>2.1 Compare and contrast TCP and UDP ports, protocols, and their purposes</b>	
Ports and protocols like 21 – FTP, 22 – SSH, 23 – Telnet, 25 – SMTP, 53 – DNS, 80 – HTTP, 110 – POP3, 143 – IMAP, 443 – HTTPS, 3389 – RDP, 137-139 – NetBIOS/NetBT, 445 – SMB/CIFS, 427 – SLP, 548 – AFP, 67/68 – DHCP, 389 – LDAP, and 161/162 – SNMP	<a href="#">8-3</a>
TCP versus UDP	<a href="#">8-3</a>
<b>2.2 Compare and contrast common networking hardware devices</b>	
Devices like Routers, Switches (Managed, and Unmanaged), Access points, Cloud-based network controller, Firewall, Network interface card, Repeater, Hub, Cable/DSL modem, Bridge, Patch panel, Power over Ethernet (PoE) (Injectors or Switch), Ethernet over Power	<a href="#">8-1</a>
<b>2.3 Given a scenario, install and configure a basic wired/wireless SOHO network</b>	
Router/switch functionality	<a href="#">8-4</a>
Access point settings	<a href="#">8-4</a>
IP addressing	<a href="#">8-4</a>
NIC configuration, Wired, Wireless	<a href="#">8-4</a>
End-user device configuration	<a href="#">8-4</a>
IoT device configuration like Thermostat, Light switches, Security cameras, Door locks, Voice-enabled, and smart speaker/digital assistant	<a href="#">8-4</a>

<b>Domain/Objective/Description</b>	<b>Book-Chapter</b>
Cable/DSL modem configuration	<a href="#">8-4</a>
Firewall settings like DMZ, Port forwarding, NAT, UPnP, Whitelist/blacklist, and MAC filtering	<a href="#">8-4</a>
QoS	<a href="#">8-4</a>
Wireless settings, Encryption, Channels, QoS	<a href="#">8-4</a>
<b>2.4 Compare and contrast wireless networking protocols</b>	
Protocols including: 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac	<a href="#">8-2</a>
Frequencies including 2.4Ghz, and 5Ghz	<a href="#">8-2</a>
Channels, 1–11	<a href="#">8-2</a>
Other wireless technologies including: Bluetooth, NFC, RFID, Zigbee, Z-Wave, 3G, 4G, 5G, LTE	<a href="#">8-2</a>
<b>2.5 Summarize the properties and purposes of services provided by networked hosts</b>	
Server roles like Web server, File server, Print server, DHCP server, DNS server, Proxy server, Mail server, Authentication server, and syslog	<a href="#">8-1</a>
Internet appliance like UTM, IDS, IPS, and End-point management server	<a href="#">8-1</a>
Legacy/embedded systems	<a href="#">8-1</a>
<b>2.6 Explain common network configuration concepts</b>	
IP addressing like Static, Dynamic, APIPA, and Link local	<a href="#">8-3</a>
DNS	<a href="#">8-3</a>
DHCP, Reservations	<a href="#">8-3</a>
IPv4 versus IPv6	<a href="#">8-3</a>
Subnet mask	<a href="#">8-3</a>
Gateway	<a href="#">8-3</a>
VPN	<a href="#">8-3</a>
VLAN	<a href="#">8-3</a>
NAT	<a href="#">8-3</a>
<b>2.7 Compare and contrast Internet connection types, network types, and their features</b>	



<b>Domain/Objective/Description</b>	<b>Book-Chapter</b>
Internet connection types, Cable, DSL, Dial-up, Fiber, Satellite, ISDN, Cellular (Tethering and Mobile hotspot, Line-of-sight wireless Internet service)	<a href="#">8-4</a>
Network types like LAN, WAN, PAN, MAN, and WMN	<a href="#">8-1</a>
<b>2.8 Given a scenario, use appropriate networking tools</b>	
Tools include: Crimper, Cable stripper, Multimeter, Tone generator and probe, Cable tester, Loopback plug, Punchdown tool, WiFi analyzer	<a href="#">8-1</a>
<b>3.0 Hardware</b>	
<b>3.1 Explain basic cable types, features, and their purposes</b>	
Network cables including Ethernet (Cat 5 – 6, Plenum, Shielded twisted pair, Unshielded twisted pair, and 568A/B), Fiber, Coaxial, Speed and transmission limitations	<a href="#">8-1</a>
Video cables like VGA, HDMI, Mini-HDMI, DisplayPort, and DVI (DVI-D/DVI-I)	<a href="#">3-1</a>
Multipurpose cables like Lightning, Thunderbolt, USB, USB-C, USB 2.0, and USB 3.0	<a href="#">3-1</a>
Peripheral cables like Serial	<a href="#">3-1</a>
Hard drive cables like SATA, IDE, SCSI	<a href="#">3-1</a>
Adapters like DVI to HDMI, USB to Ethernet, DVI to VGA	<a href="#">3-1</a>
<b>3.2 Identify common connector types</b>	
RJ-11, RJ-45, BNC, RG-59, RG-6	<a href="#">8-1</a>
RS-232, USB, Micro-USB, Mini-USB, USB-C, DB-9, Lightning, SCSI, eSATA, Molex	<a href="#">3-1</a>
<b>3.3 Given a scenario, install RAM types</b>	
RAM types like SODIMM, DDR2, DDR3, and DDR4	<a href="#">2-3</a>
Memory types including: Single channel, Dual channel, Triple channel	<a href="#">2-3</a>
Error correcting like Parity versus non-parity	<a href="#">2-3</a>
<b>3.4 Given a scenario, select, install and configure storage devices</b>	
Optical drives like CD-ROM/CD-RW, DVD-ROM/DVD-RW/DVD-RW DL, Blu-ray, BD-R, and BD-RE	<a href="#">2-5</a>
Solid state drives like M2 drives, NVME, SATA 2.5	<a href="#">2-5</a>
Magnetic hard drives like 5,400rpm, 7,200rpm, 10,000rpm, and 15,000rpm	<a href="#">2-5</a>

<b>Domain/Objective/Description</b>	<b>Book-Chapter</b>
Sizes: 2.5 and 3.5	<a href="#">2-5</a>
Hybrid drives	<a href="#">2-5</a>
Flash like SD card, CompactFlash, Micro-SD card, Mini-SD card, and xD	<a href="#">2-5</a>
Configurations like RAID 0, 1, 5, 10, and Hot swappable	<a href="#">2-5</a>
<b>3.5 Given a scenario, install and configure motherboards, CPUs, and add-on cards</b>	
Motherboard form factors like ATX, mATX, ITX, and mITX	<a href="#">2-1</a>
Motherboard connectors types like PCI, PCIe, Riser card, Socket types, SATA, IDE, Front panel connector, and Internal USB connector	<a href="#">2-1</a>
BIOS/UEFI settings like Boot options, Firmware updates, Security settings, Interface configurations, Security (Passwords, Drive encryption: TPM, LoJack, Secure boot)	<a href="#">2-4</a>
CMOS battery	<a href="#">2-1</a>
CPU features like Single-core, Multicore, Virtualization, Hyperthreading, Speeds, Overclocking, and Integrated GPU	<a href="#">2-2</a>
Compatibility: AMD, and Intel	<a href="#">2-2</a>
Cooling mechanism like Fans, Heat sink, Liquid, and Thermal paste	<a href="#">2-2</a>
Expansion cards like Video cards (Onboard or Add-on card), Sound cards, Network interface card, USB expansion card, and eSATA card	<a href="#">2-1</a>
<b>3.6 Explain the purposes and uses of various peripheral types</b>	
Devices such as Mouse, Keyboard, Touchpad, Signature pad, KVM, Magnetic reader/chip reader, NFC/tap pay device, and Smart card reader	<a href="#">3-2</a>
Devices such as Monitors, Speakers	<a href="#">3-3</a>
Devices such as Printer	<a href="#">3-4</a>
Devices such as ADF/flatbed scanner, Barcode scanner/QR scanner, VR headset, Game controllers, Camera/webcam, Microphone, Headset, Projector (Lumens/brightness)	<a href="#">3-5</a>
Devices such as Optical drive types, External storage drives	<a href="#">2-5</a>
<b>3.7 Summarize power supply types and features</b>	
Input 115V versus 220V	<a href="#">2-6</a>
Output 5V versus 12V	<a href="#">2-6</a>

<b>Domain/Objective/Description</b>	<b>Book-Chapter</b>
24-pin motherboard adapter	<a href="#">2-6</a>
Wattage rating	<a href="#">2-6</a>
Number of devices/types of devices to be powered	<a href="#">2-6</a>
<b>3.8 Given a scenario, select and configure appropriate components for a custom PC configuration to meet customer specifications or needs</b>	
Graphic/CAD/CAM design workstation including features: SSD, High-end video, Maximum RAM	<a href="#">5-1</a>
Audio/video editing workstation including features: Specialized audio and video card, Large, fast hard drive, Dual monitors	<a href="#">5-1</a>
Virtualization workstation including features: Maximum RAM and CPU cores	<a href="#">5-1</a>
Gaming PC including features: SSD, High-end video/specialized GPU, High-definition sound card, High-end cooling	<a href="#">5-1</a>
Network attached storage device including features: Media streaming, File sharing, Gigabit NIC, RAID array, Hard drive	<a href="#">5-1</a>
Standard thick client including features: Desktop applications, Meets recommended requirements for selected OS	<a href="#">5-1</a>
Thin client including features: Basic applications, Meets minimum requirements for selected OS	<a href="#">5-1</a>
Network connectivity	<a href="#">5-1</a>
<b>3.9 Given a scenario, install and configure common devices</b>	
Desktop types, including: Thin client, Thick client, Account setup/settings	<a href="#">5-1</a>
Laptop/common mobile devices, Touchpad configuration, Touchscreen configuration, Application installations/configurations, Synchronization settings, Account setup/settings, and Wireless settings	<a href="#">3-6</a>
<b>3.10. Given a scenario, configure SOHO multifunction devices/printers and settings</b>	
Use appropriate drivers for a given operating system	<a href="#">3-4</a>
Configuration settings, Duplex, Collate, Orientation, and Quality	<a href="#">3-4</a>
Device sharing over Wired (USB, Serial, Ethernet), and Wireless (Bluetooth, 802.11(a, b, g, n, ac), Infrastructure versus ad hoc	<a href="#">3-4</a>
Integrated print server (hardware)	<a href="#">3-4</a>
Cloud printing/remote printing	<a href="#">3-4</a>

<b>Domain/Objective/Description</b>	<b>Book-Chapter</b>
Public/shared devices like Sharing local/networked device via operating system settings (TCP/Bonjour/AirPrint), Data privacy (User authentication on the device, Hard drive caching)	<a href="#">8-3</a>
<b>3.11. Given a scenario, install and maintain various print technologies</b>	
Laser like Imaging drum, fuser assembly, transfer belt, transfer roller, pickup rollers, separate pads, duplexing assembly, Imaging process: processing, charging, exposing, developing, transferring, fusing, and cleaning, and Maintenance: Replace toner, apply maintenance kit, calibrate, clean	<a href="#">3-4</a>
Inkjet like Ink cartridge, print head, roller, feeder, duplexing assembly, carriage, and belt, Calibrate, and Maintenance: Clean heads, replace cartridges, calibrate, clear jams	<a href="#">3-4</a>
Thermal like Feed assembly, heating element, Special thermal paper, and Maintenance: Replace paper, clean heating element, remove debris	<a href="#">3-4</a>
Impact like Print head, ribbon, tractor feed, Impact paper, and Maintenance: Replace ribbon, replace print head, replace paper	<a href="#">3-4</a>
Virtual like Print to file, Print to PDF, Print to XPS, and Print to image	<a href="#">3-4</a>
3D printers like Plastic filament	<a href="#">3-4</a>
<b>4.0 Virtualization and Cloud Computing</b>	
<b>4.1 Compare and contrast cloud computing concepts</b>	
Common cloud models like IaaS, SaaS, PaaS, Public vs. private vs. and hybrid versus community	<a href="#">5-2</a>
Shared resources like Internal versus external	<a href="#">5-2</a>
Features like Rapid elasticity, On-demand, Resource pooling, Measured service, and Metered	<a href="#">5-2</a>
Off-site email applications	<a href="#">5-2</a>
Cloud file storage services and Synchronization apps	<a href="#">5-2</a>
Virtual application streaming/cloud-based applications including Applications for cell phones/tablets and Applications for laptops/desktops	<a href="#">5-2</a>
Virtual desktop and Virtual NIC	<a href="#">5-2</a>
<b>4.2 Given a scenario, set up and configure client-side virtualization</b>	
Purpose of virtual machines	<a href="#">5-2</a>
Resource requirements	<a href="#">5-2</a>

<b>Domain/Objective/Description</b>	<b>Book-Chapter</b>
Emulator requirements	<a href="#">5-2</a>
Security requirements	<a href="#">5-2</a>
Network requirements	<a href="#">5-2</a>
Hypervisor	<a href="#">5-2</a>
<b>5.0 Hardware and Network Troubleshooting</b>	
<b>5.1 Given a scenario, use the best practice methodology to resolve problems</b>	
Always consider corporate policies, procedures, and impacts before implementing changes	<a href="#">1-2</a>
Identify the problem using Question the user / identify user changes to computer / perform backups before making changes, Inquire regarding environmental or infrastructure changes, and Review system and application logs	<a href="#">1-2</a>
Establish a theory of probable cause (question the obvious) and If necessary, conduct external or internal research based on symptoms	<a href="#">1-2</a>
Test the theory to determine cause including Once the theory is confirmed, determine the next steps to resolve problem, or If theory is not confirmed re-establish new theory or escalate	<a href="#">1-2</a>
Establish a plan of action to resolve the problem and implement the solution	<a href="#">1-2</a>
Verify full system functionality and, if applicable, implement preventive measures	<a href="#">1-2</a>
Document findings, actions, and outcomes	<a href="#">1-2</a>
<b>5.2 Given a scenario, troubleshoot problems related to motherboards, RAM, CPUs, and power</b>	
Common symptoms including: Unexpected shutdowns, System lockups, POST code beeps, Blank screen on bootup, BIOS time and setting resets, Attempts to boot to incorrect device, Continuous reboots, No power, Overheating, Loud noise, Intermittent device failure, Fans spin – no power to other devices, Indicator lights, Smoke, Burning smell, Proprietary crash screens, (BSOD/pin wheel), Distended capacitors, and Log entries and error messages	<a href="#">4-2</a>
<b>5.3 Given a scenario, troubleshoot hard drives and RAID arrays</b>	

<b>Domain/Objective/Description</b>	<b>Book-Chapter</b>
Common symptoms including: Read/write failure, Slow performance, Loud clicking noise, Failure to boot, Drive not recognized, OS not found, RAID not found, RAID stops working, Proprietary crash screens, (BSOD/pin wheel), and S.M.A.R.T. errors	<a href="#">2-5</a>
<b>5.4 Given a scenario, troubleshoot video, projector, and display issues</b>	
Common symptoms including: VGA mode, No image on screen, Overheat shutdown, Dead pixels, Artifacts, Incorrect color patterns, Dim image, Flickering image, Distorted image, Distorted geometry, Burn-in, and Oversized images and icons	<a href="#">3-3</a>
<b>5.5 Given a scenario, troubleshoot common mobile device issues while adhering to the appropriate procedures</b>	
Common symptoms including: No display, Dim display, Flickering display, Sticking keys, Intermittent wireless, Battery not charging, Ghost cursor/pointer drift, No power, Num lock indicator lights, No wireless connectivity, No Bluetooth connectivity, Cannot display to external monitor, Touchscreen non-responsive, Apps not loading, Slow performance, Unable to decrypt email, Extremely short battery life, Overheating, Frozen system, No sound from speakers, GPS not functioning, and Swollen battery	<a href="#">3-6</a>
Disassembling processes for proper reassembly including: Document and label cable and screw locations, Organize parts, Refer to manufacturer resources, and Use appropriate hand tools	<a href="#">3-6</a>
<b>5.6 Given a scenario, troubleshoot printers</b>	
Common symptoms including: Streaks, Faded prints, Ghost images, Toner not fused to the paper, Creased paper, Paper not feeding, Paper jam, No connectivity, Garbled characters on paper, Vertical lines on page, Backed-up print queue, Low memory errors, Access denied, Printer will not print, Color prints in wrong print color, Unable to install printer, Error codes, Printing blank pages, No image on printer display, and Multiple failed jobs in logs	<a href="#">3-4</a>
<b>5.7 Given a scenario, troubleshoot common wired and wireless network problems</b>	
Common symptoms including: Limited connectivity, Unavailable resources (Internet or Local resources such as Shares, Printers, and Email), No connectivity, APIPA/link local address, Intermittent connectivity, IP conflict, Slow transfer speeds	<a href="#">8-1</a>
Common symptoms including: Low RF signal, and SSID not found	<a href="#">8-2</a>

# 2019 Examination Objectives — 220-1002 Practical Application

<b>Domain/Objective/Description</b>	<b>Book-Chapter</b>
<b>1.0 Operating Systems</b>	
<b>1.1. Compare and contrast common operating system types and their purposes</b>	
32-bit versus 64-bit, RAM limitations, Software compatibility	<a href="#">5-1</a>
Workstation operating systems, Microsoft Windows, Apple Macintosh OS, Linux	<a href="#">5-1</a>
Cell phone/tablet operating systems, Microsoft Windows, Android, iOS, Chrome OS	<a href="#">3-6</a>
Vendor-specific limitations, End-of-life, Update limitations	<a href="#">5-1</a>
Compatibility concerns between operating systems	<a href="#">5-1</a>
<b>1.2. Compare and contrast features of Microsoft Windows versions</b>	
Versions such as: Windows 7, Windows 8, Windows 8.1, Windows 10	<a href="#">5-1</a>
Corporate versus personal needs, Domain access, BitLocker, Media center, BranchCache, EFS	<a href="#">5-1</a>
Desktop styles/user interface	<a href="#">5-1</a>
<b>1.3. Summarize general OS installation considerations and upgrade methods</b>	
Boot methods, Optical disc (CD-ROM, DVD, Blu-ray), External drive/flash drive (USB/eSATA), Network boot (PXE), Internal fixed disk (HDD/SSD), Internal hard drive (partition)	<a href="#">5-3</a>
Type of installations, Unattended installation, In-place upgrade, Clean install, Repair installation, Multiboot, Remote network installation, Image deployment, Recovery partition, Refresh/restore	<a href="#">5-3</a>
Partitioning, Dynamic, Basic, Primary, Extended, Logical, GPT	<a href="#">5-3</a>
File system types/formatting, ExFAT, FAT32, NTFS, CDFS, NFS, ext3, ext4, HFS, Swap partition, Quick format versus full format	<a href="#">5-3</a>
Load alternate third-party drivers when necessary	<a href="#">5-3</a>

<b>Domain/Objective/Description</b>	<b>Book-Chapter</b>
Workgroup versus Domain setup	<a href="#">5-3</a>
Time/date/region/language settings	<a href="#">5-3</a>
Driver installation, software, and Windows updates	<a href="#">5-3</a>
Factory recovery partition	<a href="#">5-3</a>
Properly formatted boot drive with the correct partitions/format	<a href="#">5-3</a>
Prerequisites/hardware compatibility	<a href="#">5-3</a>
Application compatibility	<a href="#">5-3</a>
OS compatibility/upgrade path	<a href="#">5-3</a>
<b>1.4. Given a scenario, use appropriate Microsoft command line tools</b>	
Navigation (dir, cd, ..), shutdown, dism, sfc, chkdsk, diskpart, taskkill, gpupdate, gpresult, format, copy, xcopy, robocopy, net use, net user, [command name] /?	<a href="#">5-5</a>
Commands available with standard privileges versus administrative privileges	<a href="#">5-5</a>
ipconfig, ping, tracert, netstat, nslookup	<a href="#">5-5</a>
<b>1.5. Given a scenario, use Microsoft operating system features and tools</b>	
Administrative, Computer Management, Device Manager, Local Users and Groups, Local Security Policy, Performance Monitor, Services, System Configuration, Task Scheduler, Component Services, Data Sources, Print Management, Windows Memory Diagnostics, Windows Firewall Advanced Security, Event Viewer, User Account Management	<a href="#">6-4</a>
MSConfig, General, Boot, Services, Startup, Tools	<a href="#">6-4</a>
Task Manager, Applications, Processes, Performance, Networking, Users	<a href="#">6-4</a>
Disk Management, Drive status (Mounting, Initializing, Extending partitions, Splitting partitions, Shrink partitions, Assigning/changing drive letters, Adding drives, Adding arrays, Storage spaces)	<a href="#">6-4</a>
System utilities, Regedit, Command, Services.msc, MMC, MSTSC, Notepad, Explorer, Msinfo32, Dxdiag, Disk Defragmenter, System Restore, Windows Update	<a href="#">6-4</a>
<b>1.6. Given a scenario, use Microsoft Windows Control Panel utilities</b>	
Internet Options, Connections, Security, General, Privacy, Programs, Advanced	<a href="#">8-4</a>
Display/Display Settings, Resolution, Color depth, Refresh rate	<a href="#">5-2</a>
User Accounts	<a href="#">5-2</a>



<b>Domain/Objective/Description</b>	<b>Book-Chapter</b>
Folder Options, View hidden files, Hide extensions, General options, View options	<a href="#">5-2</a>
System, Performance (virtual memory), Remote settings, System protection	<a href="#">5-2</a>
Windows Firewall	<a href="#">5-2</a>
Power Options, Hibernate, Power plans, Sleep/suspend, Standby	<a href="#">5-2</a>
Other Control Panels such as: Credential Manager, Programs and features, HomeGroup, Devices and Printers, Sound, Troubleshooting, Network and Sharing Center, Device Manager, BitLocker, Sync Center	<a href="#">5-2</a>
<b>1.7. Summarize application installation and configuration concepts</b>	
System requirements, Drive space, RAM	<a href="#">6-2</a>
OS requirements, Compatibility	<a href="#">6-2</a>
Methods of installation and deployment, Local (CD/USB), Network-based	<a href="#">6-2</a>
Local user permissions, Folder/file access for installation	<a href="#">6-2</a>
Security considerations, Impact to device, Impact to network	<a href="#">6-2</a>
<b>1.8. Given a scenario, configure Microsoft Windows networking on a client/desktop</b>	
HomeGroup versus Workgroup	<a href="#">8-3</a>
Domain setup	<a href="#">8-3</a>
Network shares/administrative shares/mapping drives	<a href="#">8-3</a>
Printer sharing versus network printer mapping	<a href="#">8-3</a>
Establish networking connections, VPN, Dial-ups, Wireless, Wired, WWAN (Cellular)	<a href="#">8-3</a>
Proxy settings	<a href="#">8-3</a>
Remote Desktop Connection	<a href="#">8-3</a>
Remote Assistance	<a href="#">8-3</a>
Home versus Work versus Public network settings	<a href="#">8-3</a>
Firewall settings, Exceptions, Configuration, Enabling/disabling Windows Firewall	<a href="#">8-3</a>
Configuring an alternative IP address in Windows, IP addressing, Subnet mask, DNS, Gateway	<a href="#">8-3</a>

<b>Domain/Objective/Description</b>	<b>Book-Chapter</b>
Network card properties, Half duplex/full duplex/auto, Speed, Wake-on-LAN, QoS, BIOS (on-board NIC)	<a href="#">8-3</a>
<b>1.9. Given a scenario, use features and tools of the Mac OS and Linux client/desktop operating systems</b>	
Best practices, Scheduled backups, Scheduled disk maintenance, System updates/App Store, Patch management, Driver/firmware updates, Antivirus/Anti-malware updates	<a href="#">5-1</a>
Tools, Backup/Time Machine, Restore/Snapshot, Image recovery, Disk maintenance utilities, Shell/Terminal, Screen sharing, Force Quit	<a href="#">5-1</a>
Features, Multiple desktops/Mission Control, Key Chain, Spot Light, iCloud, Gestures, Finder, Remote Disc, Dock, Boot Camp	<a href="#">5-1</a>
Basic Linux commands, ls, grep, cd, shutdown, pwd vs. passwd, mv, cp, rm, chmod, chown, iwconfig/ifconfig, ps, su/sudo, apt-get, vi, dd, kill	<a href="#">5-1</a>
<b>2.0 Security</b>	
<b>2.1. Summarize the importance of physical security measures</b>	
Measures, such as: Mantrap, Badge reader, Smart card, Security guard, Door lock, Biometric locks, Hardware tokens, Cable locks, Server locks, USB locks, Privacy screen, Key fobs, Entry control roster	<a href="#">9-1</a>
<b>2.2. Explain logical security concepts</b>	
Concepts such as: Active Directory (Login script, Domain, Group Policy/Updates, Organizational Units, Home Folder, Folder redirection), Software tokens, MDM policies, Port security, MAC address filtering, Certificates, Principle of least privilege	<a href="#">9-2</a>
Concepts such as: Antivirus/Anti-malware, Firewalls, User authentication/strong passwords, Multifactor authentication, Directory permissions, VPN, DLP, Access control lists, Smart card, Email filtering, Trusted/untrusted software sources	<a href="#">9-1</a>
<b>2.3. Compare and contrast wireless security protocols and authentication methods</b>	
Protocols and encryption, WEP, WPA, WPA2, TKIP, AES	<a href="#">8-2</a>
Authentication, Single-factor, Multifactor, RADIUS, TACACS	<a href="#">8-2</a>
<b>2.4. Given a scenario, detect, remove, and prevent malware using appropriate tools and methods</b>	

<b>Domain/Objective/Description</b>	<b>Book-Chapter</b>
Malware, Ransomware, Trojan, Keylogger, Rootkit, Virus, Botnet, Worm, Spyware	<a href="#">9-3</a>
Tools and methods, Antivirus, Anti-malware, Recovery console, Backup/restore, End user education, Software firewalls, DNS configuration	<a href="#">9-3</a>
<b>2.5. Compare and contrast social engineering, threats, and vulnerabilities</b>	
Items include: Social engineering (Phishing, Spear phishing, Impersonation, Shoulder surfing, Tailgating, Dumpster diving), DDoS, DoS, Zero-day, Man-in-the-middle, Brute force, Dictionary, Rainbow table, Spoofing, Non-compliant systems, Zombie	<a href="#">9-1</a>
<b>2.6. Compare and contrast the differences of basic Microsoft Windows OS security settings</b>	
User and groups, Administrator, Power user, Guest, Standard user	<a href="#">9-2</a>
NTFS versus share permissions, Allow versus deny, Moving versus copying folders and files, File attributes	<a href="#">9-2</a>
Shared files and folders, Administrative shares versus local shares, Permission propagation, Inheritance	<a href="#">9-2</a>
System files and folders	<a href="#">9-2</a>
User authentication, Single sign-on	<a href="#">9-2</a>
Run as administrator versus standard user	<a href="#">9-2</a>
BitLocker	<a href="#">9-2</a>
BitLocker To Go	<a href="#">9-2</a>
EFS	<a href="#">9-2</a>
<b>2.7. Given a scenario, implement security best practices to secure a workstation</b>	
Password best practices, Setting strong passwords, Password expiration, Screensaver required password, BIOS/UEFI passwords, Requiring passwords	<a href="#">9-1</a>
Account management, Restricting user permissions, Logon time restrictions, Disabling guest account, Failed attempts lockout, Timeout/screen lock, Change default admin user account/password, Basic Active Directory functions (Account creation, Account deletion, Password reset/unlock account, Disable account)	<a href="#">9-1</a>
Disable autorun	<a href="#">9-2</a>

<b>Domain/Objective/Description</b>	<b>Book-Chapter</b>
Data encryption	<a href="#">9-2</a>
Patch/update management	<a href="#">9-2</a>
<b>2.8. Given a scenario, implement methods for securing mobile devices</b>	
Methods include: Screen locks (Fingerprint lock, Face lock, Swipe lock, Passcode lock), Remote wipes, Locator applications, Remote backup applications, Failed login attempts restrictions, Antivirus/Anti-malware, Patching/OS updates, Biometric authentication, Full device encryption, Multifactor authentication, Authenticator applications, Trusted sources versus untrusted sources, Firewalls, Policies and procedures (BYOD versus corporate-owned, Profile security requirements)	<a href="#">3-6</a>
<b>2.9. Given a scenario, implement appropriate data destruction and disposal methods</b>	
Physical destruction, Shredder, Drill/hammer, Electromagnetic (Degaussing), Incineration, Certificate of destruction	<a href="#">9-1</a>
Recycling or repurposing best practices, Low-level format versus standard format, Overwrite, Drive wipe	<a href="#">9-1</a>
<b>2.10. Given a scenario, configure security on SOHO wireless and wired networks</b>	
Wireless-specific, Changing default SSID, Setting encryption, Disabling SSID broadcast, Antenna and access point placement, Radio power levels, WPS	<a href="#">8-2</a>
Other items, including: Change default usernames and passwords, Enable MAC filtering, Assign static IP addresses, Firewall settings, Port forwarding/mapping, Disabling ports, Content filtering/parental controls, Update firmware, Physical security	<a href="#">8-2</a>
<b>3.0 Software Troubleshooting</b>	
<b>3.1. Given a scenario, troubleshoot Microsoft Windows OS problems</b>	
Common symptoms, Slow performance, Limited connectivity, Failure to boot, No OS found, Application crashes, Blue screens, Black screens, Printing issues, Services fail to start, Slow bootup, Slow profile load	<a href="#">7-2</a>
Common solutions, Defragment the hard drive, Reboot, Kill tasks, Restart services, Update network settings, Reimage/reload OS, Roll back updates, Roll back device drivers, Apply updates, Repair application, Update boot order, Disable Windows services/applications, Disable application startup, Safe boot, Rebuild Windows profiles	<a href="#">7-2</a>
<b>3.2. Given a scenario, troubleshoot and resolve PC security issues</b>	

<b>Domain/Objective/Description</b>	<b>Book-Chapter</b>
Common symptoms, Pop-ups, Browser redirection, Security alerts, Slow performance, Internet connectivity issues, PC/OS lockup, Application crash, OS updates failures, Rogue antivirus, Spam, Renamed system files, Disappearing files, File permission changes, Hijacked email(Responses from users regarding email, Automated replies from unknown sent email), Access denied, Invalid certificate (trusted root CA), System/application log errors	<a href="#">9-3</a>
<b>3.3. Given a scenario, use best practice procedures for malware removal</b>	
Identify and research malware symptoms	<a href="#">9-3</a>
Quarantine the infected systems	<a href="#">9-3</a>
Disable System Restore (in Windows)	<a href="#">9-3</a>
Remediate the infected systems like Update the anti-malware software, and Scan and use removal techniques (safe mode, pre-installation environment)	<a href="#">9-3</a>
Schedule scans and run updates	<a href="#">9-3</a>
Enable System Restore and create a restore point (in Windows)	<a href="#">9-3</a>
Educate the end user	<a href="#">9-3</a>
<b>3.4. Given a scenario, troubleshoot mobile OS and application issues</b>	
Common symptoms, Dim display, Intermittent wireless, No wireless connectivity, No Bluetooth connectivity, Cannot broadcast to external monitor, Touchscreen non-responsive, Apps not loading, Slow performance, Unable to decrypt email, Extremely short battery life, Overheating, Frozen system, No sound from speakers, Inaccurate touch screen response, System lockout, App log errors	<a href="#">3-6</a>
<b>3.5. Given a scenario, troubleshoot mobile OS and application security issues</b>	
Common symptoms, Signal drop/weak signal, Power drain, Slow data speeds, Unintended WiFi connection, Unintended Bluetooth pairing, Leaked personal files/data, Data transmission over limit, Unauthorized account access, Unauthorized location tracking, Unauthorized camera/microphone activation, High resource utilization	<a href="#">9-1</a>
<b>4.0 Operational Procedures</b>	
<b>4.1. Compare and contrast best practices associated with types of documentation</b>	
Items include: Network topology diagrams, Knowledge base/articles, Incident documentation, Regulatory and compliance policy, Acceptable use policy, Password policy, Inventory management (Asset tags, and Barcodes)	<a href="#">1-2</a>

<b>Domain/Objective/Description</b>	<b>Book-Chapter</b>
<b>4.2. Given a scenario, implement basic change management best practices</b>	
Items include: Documented business processes, Purpose of the change, Scope the change, Risk analysis, Plan for change, End-user acceptance, Change board (Approvals), Backout plan, Document changes	<a href="#">1-2</a>
<b>4.3. Given a scenario, implement basic disaster prevention and recovery methods</b>	
Backup and recovery (Image level, File level, and Critical applications), Backup testing, UPS, Surge protector, Cloud storage versus local storage backups, Account recovery options	<a href="#">7-3</a>
<b>4.4. Explain common safety procedures</b>	
Equipment grounding	<a href="#">1-3</a>
Proper component handling and storage, Antistatic bags, ESD straps, ESD mats, Self-grounding	<a href="#">1-3</a>
Toxic waste handling, Batteries, Toner, CRT, Cell phones, Tablets	<a href="#">1-3</a>
Personal safety, Disconnect power before repairing PC, Remove jewelry, Lifting techniques, Weight limitations, Electrical fire safety, Cable management, Safety goggles, Air filter mask	<a href="#">1-3</a>
Compliance with government regulations	<a href="#">1-3</a>
<b>4.5. Explain environmental impacts and appropriate controls</b>	
MSDS documentation for handling and disposal	<a href="#">1-3</a>
Temperature, humidity level awareness, and proper ventilation	<a href="#">1-3</a>
Power surges, brownouts, and blackouts, Battery backup, Surge suppressor	<a href="#">1-3</a>
Protection from airborne particles, Enclosures, Air filters/mask	<a href="#">1-3</a>
Dust and debris, Compressed air, Vacuums	<a href="#">1-3</a>
Compliance to government regulations	<a href="#">1-3</a>
<b>4.6. Explain the processes for addressing prohibited content/activity, and privacy, licensing, and policy concepts</b>	
Incident response, First response (Identify, Report through proper channels, Data/device preservation), Use of documentation/documentation changes, Chain of custody (Tracking of evidence/documenting process)	<a href="#">9-1</a>

<b>Domain/Objective/Description</b>	<b>Book-Chapter</b>
Licensing/DRMEULA, Open-source versus commercial license, Personal license versus enterprise licenses	<a href="#">9-1</a>
Regulated data, PII, PCI, GDPR, PHI	<a href="#">9-1</a>
Follow all policies and security best practices	<a href="#">9-1</a>
<b>4.7. Given a scenario, use proper communication techniques and professionalism</b>	
Use proper language and avoid jargon, acronyms, and slang, when applicable	<a href="#">1-2</a>
Maintain a positive attitude/project confidence	<a href="#">1-2</a>
Actively listen (taking notes) and avoid interrupting the customer	<a href="#">1-2</a>
Be culturally sensitive, Use appropriate professional titles, when applicable	<a href="#">1-2</a>
Be on time (if late, contact the customer), Avoid distractions, Personal calls, Texting/social media sites, Talking to coworkers while interacting with customers, Personal interruptions	<a href="#">1-2</a>
Dealing with difficult customers or situations, Do not argue with customers and/or be defensive, Avoid dismissing customer problems, Avoid being judgmental, Clarify customer statements (ask open-ended questions to narrow the scope of the problem, restate the issue, or question to verify understanding), Do not disclose experiences via social media outlets	<a href="#">1-2</a>
Set and meet expectations/timeline and communicate status with the customer, Offer different repair/ replacement options, if applicable, Provide proper documentation on the services provided, Follow up with customer/user at a later date to verify satisfaction	<a href="#">1-2</a>
Deal appropriately with customers' confidential and private materials, Located on a computer, desktop, printer, and so forth	<a href="#">1-2</a>
<b>4.8. Identify the basics of scripting</b>	
Script file types, .bat, .ps1, .vbs, .sh, .py, .js	<a href="#">6-5</a>
Environment variables	<a href="#">6-5</a>
Comment syntax	<a href="#">6-5</a>
Basic script constructs, Basic loops, Variables	<a href="#">6-5</a>
Basic data types, Integers, Strings	<a href="#">6-5</a>
<b>4.9. Given a scenario, use remote access technologies</b>	
RDP	<a href="#">8-3</a>

<b><i>Domain/Objective/Description</i></b>	<b><i>Book-Chapter</i></b>
Telnet	<a href="#">8-3</a>
SSH	<a href="#">8-3</a>
Third-party tools, such as: Screen share feature, File share	<a href="#">8-3</a>
Security considerations of each access method	<a href="#">8-3</a>



# Index

---

## A

absolute paths, [669](#)–672

AC adapters

laptop, [426](#)–427

overview, [426](#)–427

problems, [427](#)

troubleshooting and repair of, [427](#)

working with, [294](#)

accelerated video cards, [350](#)

acceptable use policy, [39](#)

access control lists, [1177](#)

access denied error, [392](#), [1246](#)

access points, [1019](#), [1025](#), [1136](#)

access time, hard drive, [246](#)

access token, [1161](#)–1162

account access, unauthorized, [1181](#)

account management, [1179](#)–1180

account operators, [1199](#)

Ace file, [642](#)

ACPI (Advanced Configuration and Power Interface), [423](#)

Acrylic WiFi scanner, [1026](#)

Action Center, [529](#), [577](#), [579](#), [1221](#)

Active Directory, [1180](#), [1193](#)–1194

Active Directory Database, [1160](#)

- active heat sink, [172](#)
- active matrix display, [428](#)
- Active Server Page Extended files, [644](#)
- Active Server Page files, [644](#)
- ActiveX Control (OCX) files, [807](#)
- actuator arm, [243](#)
- AD (Active Directory), [728](#)
- ad hoc mode, [386](#), [1001](#)
- adapter cards, [80](#)–81
- adapters
  - DVI to HDMI, [321](#)
  - DVI to VGA, [321](#)
  - overview, [320](#)–321
  - USB to Ethernet, [322](#)
- Ad-Aware, [1237](#)
- Add Legacy Hardware, [708](#)–709
- add-on cards, [129](#)
- address bus, [139](#)–140
- address lines, [139](#)
- address space, [738](#)
- ADK (Assessment and Deployment Kit), [685](#)
- administrative shares, [1081](#)–1082, [1210](#)–1211
- Administrative Tools, [590](#)
- Administrative Tools, Control Panel applet, [576](#)
- administrator account, [1196](#)
- Administrator Command Prompt, [667](#)
- administrator password, [223](#)–225

administrators, [1199](#), [1206](#)  
ADSL (Digital Subscriber Line), [1129](#)  
adware, [1155](#), [1237](#)–1238  
Aero Desktop, [586](#), [779](#)  
AES (Advanced Encryption Standard), [1010](#)  
AFP (Apple Filing Protocol), [1063](#), [1064](#)  
AfterStep, [533](#)  
AGP (Accelerated Graphics Port), [99](#), [122](#), [126](#)–127  
AHCI (Advanced Host Controller Interface), [232](#), [233](#)  
air filters/mask, [62](#), [68](#)  
airborne particles, [64](#), [68](#)  
airflow, [473](#)–477  
AirPrint, [375](#), [1092](#), [1093](#)  
AirSnort, [1009](#)  
alkaline batteries, [420](#)  
allow permission, [1208](#)  
alphanumeric keys, [328](#)  
ALU (arithmetic logic unit), [141](#)–142  
AMD processors, [152](#), [162](#)–165  
AMD-V (AMD Virtualization), [144](#), [231](#)  
ampere, [282](#)  
AMR (Audio/Modem Riser), [129](#)  
analog audio connector, [307](#)  
analog display, [355](#)  
Analyze Wait Chain, [766](#)  
Andreessen, Marc, [1114](#)  
Android Marketplace, [453](#)

Android OS, [443](#), [452](#)  
antenna, [1019](#)  
antiglare filter, [355](#)  
anti-malware, [944](#), [1246](#)  
antispay software, [1246](#)  
antistatic bags, [60](#)  
antistatic wrist strap, [60](#)  
antivirus software, [1225](#), [1234](#)–1235, [1242](#), [1246](#)  
API (application programming interface), [588](#)  
APIPA (Automatic Private IP Addressing), [1050](#)  
APlus, [1015](#)  
APM (Advanced Power Management), [423](#)  
App Store, [453](#), [461](#), [552](#)  
Apple MacOS. *See* [macOS](#)  
Apple Watch, [443](#)  
application layer, cloud, [597](#)  
application logs, [32](#)

## applications

16-bit, [738](#)–739

32-bit, [734](#)–738

64-bit, [735](#)–738

critical, [932](#)

installing, [726](#)–730

install/start/load errors, [744](#)

MS-DOS based, [739](#)–742

multitasking, [732](#)–734

multithreaded, [734](#)

overview, [725](#)–726

Prep Test, [746](#)–747

problems with, [910](#)–913

removing, [730](#)–731

repairing, [731](#)–732

virtual, [603](#)

Windows compatibility modes, [742](#)–743

Applications tab, Task Manager, [757](#)

apps, [726](#)

APT (Advanced Packaging Tool), [533](#)

`apt-get` command, [544](#)–545

Arc file, [642](#)

Arch Linux, [533](#)

Archive attribute, [646](#)–647, [657](#)

Archive file, [642](#)

arguments, [833](#)

.arj file, [642](#)

ARP (Address Resolution Protocol), [1060](#)–1061

ARPANET, [1104](#)

array variable type, [853](#)

artifacts, visual, [358](#)

.asp file, [644](#)

aspect ratios, [86](#), [348](#)

ASPs (application service providers), [1107](#)

.aspx file, [644](#)

association, [635](#)

Association of Better Computer Dealers, [20](#)

ATA (Advanced Technology Attachment), [78](#), [249](#), [317](#)

ATA-1 standard, [249](#)

ATAPI (ATA Packet Interface), [249](#)

Athlon 64 processor (AMD), [164](#)–165

Athlon 64 X2 processor (AMD), [164](#)–165

Athlon processor (AMD), [163](#)

Athlon XP processor (AMD), [164](#)

attack types. *See also* [malware \(malicious software\)](#)

- network-based attacks, [1148](#)–1153
- overview, [1146](#)
- social engineering attacks, [1146](#)–1148
- software-based attacks, [1153](#)–1154

attrib.exe command, [655](#)–657, [683](#)

ATX motherboard, [121](#)–122

ATX power supply, [113](#), [284](#)–285, [287](#)–293

audio ports, [94](#)

audio/video-editing system, [555](#)

- audit account logon, [1213](#)
- audit account management, [1213](#)
- audit logon events, [1213](#)
- audit object access, [1213](#)
- audit policy change, [1213](#)
- audit privilege use, [1213](#)
- audit system events, [1213](#)
- auditing, [1212](#)–1215, [1223](#)
- AUI (adapter unit interface), [968](#)
- AUP (acceptable use policy), [461](#)
- authentication
  - access token, [1160](#)–1161
  - multifactor, [1013](#), [1164](#)
  - objects, [1162](#)–1163
  - overview, [1159](#)–1160, [1193](#)
  - RADIUS, [1013](#)
  - single sign-on, [1163](#)
  - single-factor, [1013](#)
  - smart cards, [1161](#)
  - strong passwords, [1163](#)
  - TACACS, [1013](#)
  - with wireless, [1013](#)
- authentication server, [955](#)
- authorization, [1164](#)–1165
- auto lock, [1182](#)
- automatic switching, [284](#)
- automatic updates, [620](#)

Automatic Updates, [902](#)  
auto-restart errors, [900](#)–902  
autorun, disabling, [1180](#)

## ***B***

back probing, [512](#)  
backed-up print queue, [392](#)  
background printing, [383](#)  
backlight, [354](#), [446](#)  
backout plan, [42](#)–43  
backup operators, [1199](#)  
backups  
    Backup and Restore tool, [1248](#)  
    differential, [1171](#)  
    file extensions, [642](#)  
    File History, [932](#)–933  
    full, [1171](#)  
    incremental, [1172](#)  
    offsite, [1172](#)  
    overview, [931](#)–932, [1170](#)–1171  
    PC Refresh and Reset, [934](#)  
    review, [1171](#)  
    scheduling, [551](#)–552  
    System Restore, [935](#)–937  
    testing, [932](#)  
    Time Machine (macOS), [550](#)  
    in troubleshooting and good practices, [34](#)–35



badge reader, [1162](#)

.bak file, [642](#)

barcode reader, [338](#)

bash (Bourne-Again Shell), [1118](#)

basic disk, [617](#)

batch (.bat) file

- arguments, [833](#)

- choice statement, [835](#)–836

- commands, locating, [837](#)–838

- comment syntax symbol, [871](#)

- directions, [832](#)

- environment variables, [835](#)

- file extensions, [640](#)

- if statement, [834](#)–835

- looping, [836](#)–837

- overview, [830](#)

- parameters, [833](#)

- redirection symbols, [832](#)

- rem statements, [838](#)–839

## batteries

- alkaline, [420](#)
- backup, [68](#)
- changing, [421](#)
- CMOS, [102](#), [216](#), [420](#)
- disposal of, [65](#)
- handling, [421](#)
- laptop, [420](#)–422
- lithium-ion, [420](#)
- nickel-metal hydride, [420](#)
- performance, [421](#)–422
- smart, [421](#)
- swollen, [460](#)
- troubleshooting, [459](#), [509](#)–513

Battery Act, [65](#)

baud rate, [312](#), [507](#)

BCD (Boot Configuration Database), [693](#), [881](#)–882

`bcdedit.exe`, [882](#)

BD-REs (Blu-ray disc recordable erasables), [271](#)

BD-Rs (Blu-ray disc recordables), [271](#)

## best practices

- change management implementation, [41](#)–44
- communication skills, [44](#)–46
- Prep Test, [52](#)–53
- professionalism, [46](#)–50
- troubleshooting, [29](#)–40

.bhx file, [642](#)

Binhex, [642](#), [1109](#)

biometric devices, [338](#), [1159](#)–1160

BIOS (basic input-output system). *See also* [CMOS setup program](#)

- backing up settings, [35](#)
- BIOS chip, [100](#)–101, [102](#), [122](#), [210](#)
- BIOS component information, [216](#)
- versus CMOS, [83](#), [210](#)–211
- component information, [216](#)
- date and revision number, [227](#)–228
- defined, [82](#)
- passwords, [1157](#), [1174](#), [1179](#)
- physical security settings, [1157](#)
- Plug and Play, [226](#)
- Prep Test, [235](#)–239
- securing system through, [1187](#)–1189
- security features, [222](#)–226
- troubleshooting, [497](#)–499
- upgrading, [211](#)–214
- Windows installations, [619](#)

BitLocker, [587](#), [1173](#), [1224](#)

BitLocker-To-Go, [1224](#)

Bitmap, [643](#)

Black Box, [533](#)

Blackberry, [455](#)

Blackberry App World, [453](#)

black-hat hackers, [1146](#)

blacklisting, [1137](#)

- blackout, [67](#), [295](#)
- blank page, printer problems, [391](#)
- blank screen on boot, [906](#)
- blue screen errors, [902](#)–905
- Bluetooth, [339](#), [436](#)–437, [458](#), [460](#), [1021](#)–1022, [1181](#)
- Blu-ray discs, [271](#)
- .bmp file, [643](#)
- BNC connector, [967](#)–968
- BNC-T connector, [967](#)–968
- bool variable type, [854](#)
- Boolean logic, [844](#)–845
- Boolean operators, [856](#)
- Boot Camp, [550](#)
- boot devices, [1157](#), [1192](#)
- boot options, [222](#)

## boot process

- advanced options, Windows, [923](#)

- booting from Windows DVD, [610](#)

- booting off network, [228](#)–229, [611](#), [620](#)

- errors, [877](#)–884

- F8 options, [919](#)–927

- improper shutdown and boot, [926](#)–927

- Linux boot issues, [883](#)–884

- missing boot files, [879](#)–883

- overview, [691](#)

- POST process, [692](#)

- Prep Test, [700](#)–702

- problems causing reboot, [900](#)–909

- Safe Mode, [920](#)–921

- tracking the boot with bootlog, [921](#)–922

- for Windows, [692](#)–696

## boot sector virus, [1232](#)

## boot sequence, [222](#)

## bootable DVD, [222](#)

## boot.ini file, [880](#)

## bootlog, [921](#)–922

## bootmgr file, [692](#)–693, [881](#)

## BOOTREC utility, [247](#), [882](#)

## botnet, [1153](#), [1239](#)

## bottlenecks, areas of, [750](#)

## bridges, [981](#)–982

## brightness, [355](#)

British Naval Connector. *See* [BNC connector](#)

brownouts, [67](#), [295](#)

browsers, Internet

- phishing protection features, [1239](#)

- pop-up blockers, [1239](#)

- redirection of, [1244](#)

- settings, [1120](#)–1124

brute force attack, [1149](#)

BSD Unix, [534](#)

BSOD (blue screen of death), [359](#), [493](#)

buffer overflow attacks, [145](#), [1153](#)–1154

buffered memory, [194](#), [979](#)

built-in accounts, [1195](#)

built-in coprocessors, [350](#)

built-in diagnostics, [231](#)–232

burn-in, [358](#), [505](#)

burning CDs, [269](#)

burnt pixels, [505](#)

bus

- address, [139](#)–140

- data, [138](#)–139

- defined, [78](#)

- slots, [124](#)

- speed, [232](#)

- topology, [957](#)–958

## bus architectures

AGP, [126](#)–127

AMR, [129](#)

CNR, [129](#)

miniPCI, [129](#)

miniPCI Express, [129](#)

overview, [124](#)

PCI, [124](#)–125

PCIe, [128](#)

PCI-X, [127](#)

PCMCIA, [125](#)–126

Bus Enumerator, [716](#)–717

BYOD (bring your own device), [455](#), [461](#)–462

byte variable type, [853](#)

## C

CAB (Change Advisory Board), [43](#)–44

.cab file, [642](#)

Cabinet file, [642](#)

cable connections, [1128](#)–1129, [1137](#)

cable management, [62](#)

cable modem, [987](#)

cable stripper, [991](#)

cable tester, [992](#), [1073](#)

## cables

- audio, [307](#)
- coaxial, [965](#)–966
- DisplayPort, [306](#)
- DVI, [306](#)–307
- fiber optic, [969](#)–970
- hard drive, [317](#)–320
- HDMI, [305](#)
- IDE, [251](#)–252
- laplink, [989](#)
- Lightning, [308](#)
- lock, [1158](#)–1159
- mini-DisplayPort, [306](#)
- mini-HDMI, [305](#)
- multipurpose, [307](#)–312
- network, [962](#)–970
- null modem, [314](#)–315, [989](#)
- overview, [303](#)–304
- Prep Test, [323](#)–325
- SATA, [265](#), [318](#)–319
- SCSI, [260](#), [319](#)–320
- serial, [312](#)–317
- Thunderbolt, [308](#)
- troubleshooting, [970](#)–971
- twisted pair, [962](#)–963
- USB, [310](#)–312, [458](#)
- VGA, [304](#)



video, [303](#)–307

wiring standards, [963](#)–965

cache memory

defined, [141](#)

integrated, [97](#)

L1 (level 1), [195](#)

L2 (level 2), [195](#)–196

L3 (level 3), [196](#)

overview, [97](#)–98, [194](#)–195

processor, relation to, [141](#)

SRAM, [183](#)

types of, [141](#)

viewing with CPU-Z, [196](#)–197

caching, shared folder, [1077](#)

Cacti, [484](#)

calibration tests, printer, [486](#)

camcorders, [411](#)–412

camera activation, unauthorized, [1182](#)

camera resolution, [405](#)

canister, [57](#)

capacitive keyboard, [329](#)

card readers, [439](#)

carpet spray, [59](#)

carriage-and-belt system, [376](#)

cases, [84](#), [480](#)–481

cat command, [543](#)

CCD (charge-coupled device), [402](#)

`cd` (`chdir`) command, [672](#)–[673](#)  
CD Audio files, [644](#)  
`cd` command, [537](#)  
CD-/DVD-ROM drive, [442](#)  
CDFS (Compact Disc File System), [618](#)  
CDR (CD Recordable), [269](#)–[270](#)  
CD-ROM (compact disc–read-only memory), [269](#)–[270](#), [692](#)  
CD-ROM drives, [77](#)  
CD-RW (CD ReWritable), [269](#)–[270](#)  
Celeron processor (Intel), [152](#), [157](#)  
cell phones, [66](#)  
cellular cards, [337](#)  
cellular networks, [1023](#)–[1024](#), [1131](#)  
centralized administration, [953](#)  
CERN (European Council for Nuclear Research), [1105](#)  
certificate of destruction, [1169](#)  
certificates, [1194](#)  
CF (CompactFlash) cards, [272](#)  
CFX v1.62, [292](#)  
CGA (Color Graphics Adapter), [304](#), [347](#)  
chair, [70](#)  
change management process, [41](#)

## changes

- backout plan, [42](#)–43
- documenting, [44](#)
- end-user acceptance, [43](#)
- plan for, [42](#)
- purpose of, [42](#)
- risk analysis, [42](#)
- scope of, [42](#)

## channel

- T1 connection, [1130](#)
- wireless network, [1015](#)–1016, [1020](#), [1138](#)

## char variable type, [854](#)

## Cheat Sheet, explained, [6](#)

## chip extractor, [57](#)

## chip inserter, [57](#)

## chip packaging, [146](#)–147

## chipsets, [81](#)–82, [99](#)

## chkdsk.exe (Check Disk) utility, [247](#), [678](#), [790](#)–792, [944](#)

## chmod command, [539](#)

## choice statement, [835](#)–836

## chown command, [540](#)

## Chrome OS, [443](#)

## CIDR (Classless Inter-Domain Routing), [1043](#)–1044

## CIFS protocol, [1063](#), [1064](#)

## cipher.exe utility, [649](#)–650

## classification, data, [1175](#)

## cleaners, [472](#)

- cleaning blade, [370](#)
- cleaning cloths, [472](#)
- cleaning kit, [472](#)
- cleaning pads, [472](#)
- cleartext, [1166](#)
- clients, [952](#), [1025](#)
- client-server networking, [953](#)–955
- clock multipliers, [153](#), [154](#)
- clock speed, [219](#), [232](#)
- cloud computing
  - application layer, [597](#)
  - cloud file storage services, [602](#)
  - community cloud, [598](#)
  - defined, [595](#)
  - external cloud, [599](#)
  - IaaS (Infrastructure as a Service), [599](#)–600
  - internal cloud, [599](#)
  - models, [596](#)–601
  - off-site email applications, [602](#)
  - OS and middleware, [597](#)
  - overview, [598](#)
  - PaaS (Platform as a Service), [601](#)
  - physical infrastructure, [596](#)–597
  - principles, [595](#)
  - private cloud, [598](#)–599
  - public cloud, [598](#)–599
  - SaaS (Software as a Service), [601](#)

- cloud file storage services, [602](#)
- cloud-based network controller, [987](#)
- cloud-based printers, [375](#)–376
- cloud-based synchronization, [458](#)
- CloudPrint, [375](#)
- clusters, hard drive, [244](#)
- .cmd file, [640](#)
- cmd.exe, [664](#)–665
- Cmdlets, [852](#)
- CMOS (complementary metal-oxide semiconductor)
  - battery, [101](#), [216](#), [420](#)
  - versus BIOS/UEFI, [83](#), [210](#)–211
  - general discussion, [214](#)–215
  - overview, [82](#)
  - RAM, [183](#)–184
  - troubleshooting, [497](#)–499
- CMOS battery, [420](#)
- CMOS setup program
  - advanced settings, [226](#)–233
  - basic settings, [216](#)–226
  - entering, [214](#)–215
  - overview, [211](#)
- CNR (Communication and Network Riser), [129](#)
- coaxial cables, [965](#)–966
- Code Red, [902](#)
- codecs, [407](#)–408
- cold boot, [94](#)

- cold swapping, [717](#)
- color depth, [85](#), [355](#), [584](#)
- color patterns, incorrect, [358](#)
- color support, video card, [350](#)–351
- COM (communications) ports. *See* [serial ports](#)
- COM (Component Object Model), [810](#)
- .com file, [640](#)
- command file, [640](#)
- command line, [575](#), [640](#), [655](#)–657
- Command Prompt. *See also* specific commands and utilities
  - cmd.exe, [664](#)–665
  - command.com, [664](#)–665
  - directories, managing, [667](#)–673
  - overview, [576](#), [643](#)
  - Prep Test, [688](#)–689
  - privileges, executing, [665](#)–667
- command shells, [1118](#)–1119
- command.com, [664](#)–665
- commercial license, [1185](#)
- commit, [753](#)
- communication skills, [45](#)–46
- community cloud, [598](#)
- compact.exe utility, [648](#)–649
- comparison operators, PowerShell, [855](#)
- compatibility errors, [912](#)–913
- compatibility mode, [266](#), [588](#)–589, [742](#)–743
- compliance, [1174](#)

- compliance policy, [38](#)
- compliant systems, [1174](#)
- Component Services, [810](#)
- components. *See also specific components*
  - adapter cards, [80](#)–81
  - BIOS, [82](#)
  - cases, [84](#)
  - CMOS, [83](#)
  - cooling system and fans, [81](#)
  - firmware, [81](#)–82
  - I/O devices, [84](#)–86
  - memory, [79](#)
  - overview, [75](#)–76
  - power supply, [80](#)
  - Prep Test, [87](#)–90
  - processor/CPU, [76](#)–77
  - protecting, [63](#)–64
  - related, testing, [36](#)
  - storage devices, [77](#)–78
  - system boards, [80](#)
  - UEFI, [82](#)
- Compress attribute, [647](#)–649
- compressed air, [68](#), [392](#), [472](#)
- compression file extensions, [641](#)
- compression utilities, [641](#)

CompTIA A+ Certified Professional certification. *See also* [exams](#)  
    additional certifications, [6](#)  
    importance of, [19](#)–20  
    online resources, [5](#)–6  
    overview, [1](#)–4

CompTIA A+ Exam 220-1001, [23](#)–24. *See also* [exams](#)

CompTIA A+ Exam 220-1002, [23](#)–24. *See also* [exams](#)

Computer Browser service, [775](#)

computer components  
    preventive maintenance, [480](#)–481  
    swapping, [492](#)

Computer Management, [809](#)–810, [1195](#)–1197

computer name, [615](#)–616, [1084](#)–1085

computer vacuum, [472](#)

computers. *See also* [components](#)  
    functions of, [75](#)–76  
    identifying changes to, [31](#)  
    installing memory on, [199](#)  
    legacy-free, [312](#)  
    name, changing, [1054](#)–1055  
    networking, [988](#)–989

confidence, [46](#)–47

confidential information. *See* [data protection](#)

confidentiality, [47](#)

Configuration Manager, [717](#)–718



## configuration utilities

- Component Services, [810](#)

- Computer Management, [809](#)–810

- Device Manager, [807](#)–808

- overview, [799](#)

- `regsvr32.exe`, [807](#)

- Services Administrative tool, [811](#)

- System Configuration, [799](#)–801

Configurator tool, [455](#)

connectivity issues, [990](#)

connectors. *See also specific connector types*

- audio, [307](#)

- front panel, [108](#)

- keyboard/mouse, [106](#)–107

- for memory, [198](#)

- overview, [303](#)–304

- serial, [315](#)–317

- sound, [108](#)

- troubleshooting, [496](#)

content filtering, [1021](#)

continuous form feeders, [368](#)

contrast ratio, [355](#)

Control Panel, [576](#)–579, [590](#), [1197](#)–1198

Control Panel files, [642](#)

controller, [99](#)

converged devices. *See* [mobile devices](#)

cooling fans, [171](#)–172

cooling system, [81](#), [476](#)

cooperative multitasking, [732](#)–733, [738](#)

COPE (corporate owned, personally enabled), [462](#)

copy command, [674](#)

copy on write, [588](#)

Core 2/Solo/Duo/Quad, [162](#)

corporate policies, [34](#), [1186](#)

corrupted out, when printing, [388](#)

corrupted shortcuts, [910](#)–911

cp command, [538](#)

.cpl file, [642](#)

## CPU (central processing unit)

- address bus, [139](#)–140
- AMD, [162](#)–165
- architecture, [144](#)–145
- bottlenecks, [750](#)
- chip packaging, [146](#)–147
- CMOS setup program settings, [219](#)
- cooling, [169](#)–171, [476](#)
- data bus, [138](#)–139
- EDB, [145](#)
- fans, [170](#)–171
- heat sinks, [170](#)–172
- hyperthreading, [142](#)–143
- installing, [167](#)–169
- integrated GPU, [145](#)
- Intel, [152](#)–162
- match co-processor, [141](#)–142
- MMX (MultiMedia eXtensions), [142](#)
- motherboard chipset, [99](#)–100
- overclocking, [146](#)
- overview, [76](#)–77, [137](#)
- performance, increasing, [172](#)
- Prep Test, [173](#)–177
- registers, [140](#)–141
- replacing, [448](#)
- single-core vs. multicore, [142](#)–143
- socket types, [95](#), [150](#)–152, [166](#)

speed, [77](#), [138](#)  
throttling, [146](#)  
troubleshooting, [498](#)–499  
usage, [751](#)  
virtualization support, [144](#)  
voltage, [166](#)  
VRM, [146](#)

Windows systems requirements, [525](#)

CPU tab, Windows Resource Monitor, [766](#)

CPU-Z program, [188](#), [193](#), [196](#)–197

crash screens, [493](#)–494, [905](#)–906

creased paper, printer problem, [392](#)

Credential Manager, [586](#)–587

crimper, [991](#), [1073](#)

critical applications, [932](#)

cross-linked file, [791](#)

CRT (cathode ray tube) monitor, [61](#), [63](#), [64](#), [65](#)

CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance), [972](#)

CSMA/CD (Carrier Sense Multiple Access/Collision Detection), [972](#)

CSS (Cascading Style Sheet), [644](#)

cursor keys, [328](#)

customers, dealing with, [44](#)–50

cylinders, hard drive, [244](#)–245

## **D**

DAC (digital-to-audio converter), [360](#)

daemons, [1117](#)

daisy-chaining

- defined, [221](#)

- parallel port mode, [221](#)

- SCSI, [264](#), [363](#)

- USB devices, [109](#)

damaged pixels, [505](#)

damaged setting, [911](#)

DARPA (Defense Advanced Research Projects Agency), [1103](#)–1104

DAT (digital audio tape), [275](#)

.dat file, [642](#)

data bits, [507](#)

data bus, [138](#)–139, [457](#)–458

Data Collector Sets, [761](#)–764

data input, [75](#)–76. *See also* [input devices](#)

data leaks, [1181](#)

data output, [75](#)–76. *See also* [output devices](#)

data protection

- backing up data, [1170](#)–1172

- classification, [1175](#)

- compliance, [1174](#)

- data destruction and disposal, [1168](#)–1170

- encryption, [1173](#)

- overview, [1167](#)–1168

data speed, slow, [1181](#)

data transmission overlimit, [460](#)

data/device preservation, [1183](#)

dataflow analysis, [155](#)

DataVac, [472](#)

date

BIOS, [227](#)–228

CMOS setup program settings, [222](#)

Date and Time applet, [576](#)

daughter board, [80](#)

DB-25 connector, [316](#)–317

DB25-female parallel port, [105](#)

DB25-male serial port, [104](#)

DB-9 connector, [315](#)–316

DB9-male serial port, [104](#)

DC adapters, [295](#)

DC controllers, [418](#)

dd command, [546](#)

DDoS (distributed denial of service) attack, [1150](#)

DDR (double data rate) memory, [186](#)

DDR2 memory, [186](#)–187

DDR3 memory, [186](#)–187

DDR4 memory, [187](#)

DDS (Digital Data Storage), [275](#)

DD-WRT, [1012](#)

dead pixel, [358](#)

Debian, [533](#)

debris, [64](#), [68](#), [478](#)

Debugging Mode, [923](#)

decimal variable type, [854](#)

decisions, [844](#)–845

- decryption, [459](#)
- default gateway, [1044](#)–1045
- defrag.exe utility, [247](#), [678](#), [788](#)–789
- defragmentation, [788](#)–790, [944](#)
- degaussing, [358](#), [1168](#)
- deionized water, [503](#)
- del command, [677](#)
- deny permission, [1208](#)
- Dependencies tab, [777](#)
- desktop PCs, installing memory on, [199](#)
- device drivers. *See* [drivers](#)
- device load process, [694](#)–695
- Device Manager
  - accessing, [712](#)
  - device settings, changing, [711](#)
  - device-related errors, [885](#)–886
  - hardware resource settings, [710](#)–711
  - overview, [807](#)–808
- dfrgui.exe utility, [788](#)–790
- DHCP (Dynamic Host Configuration Protocol), [1012](#), [1015](#), [1016](#), [1046](#)–1048, [1063](#), [1064](#), [1133](#)
- DHCP server, [955](#)
- DHCP Server service, [1094](#)

diagnostic utilities

- DirectX Diagnostic Tool, [817](#)

- Event Viewer, [812](#)–814

- overview, [811](#)

- System File Checker, [815](#)

- System Information tool, [811](#)–812

- Windows Memory Diagnostics, [815](#)–817

dial-up, [1091](#), [1128](#)

dictionary attacks, [1149](#)

differential backups, [1171](#)

digital audio connector, [307](#)

digital cameras

- overview, [404](#)

- resolution, [405](#)–406

- uploading pictures to computer, [406](#)

- zoom, [406](#)

digital displays, [355](#)

digital security, [1176](#)–1177

digital video cameras, [407](#)

Digital Visual Interface (DVI), [306](#)–307

digital zoom, [406](#)

digitizer, [340](#), [435](#)

dim displays, [459](#)

dim image, display, [358](#)

DIMMs (dual inline memory modules), [96](#)–97, [188](#)–189

DIP (dual inline package) chips, [146](#)–147

DIP (dual inline package) switches, [118](#)–119



## directories

managing, [667](#)–673

permissions, [1177](#)

renaming, [677](#)

root, [667](#)

switches, [671](#)

directory command (`dir`), [668](#)

Directory Services Restore Mode, [923](#)

DirectX Diagnostic Tool, [817](#)

dirt, [478](#)

Disable Automatic Restart on System Failure boot option, [923](#)

disappearing files, [1245](#)

## disaster recovery

- backup and restore, [931](#)–938

- Emergency Repair Process, [927](#)–931

- F8 options during boot-up, [919](#)–927

- factory repair partition, [928](#)

- Last Known Good Configuration, [923](#)

- overview, [919](#)

- Prep Test, [946](#)–948

- preventive maintenance, [944](#)

- recovery and rescue methods, [938](#)–943

- recovery DVDs, [938](#)

- recovery image, [939](#)

- recovery partitions, [938](#)

- rescue CDs, [939](#)–941

- rescue partitions (rescue installations), [943](#)

- restore point, [936](#)–938

- startup repair, [928](#)

- system image recovery, [928](#)–931

## discoloration, [358](#)

## discretion, [47](#)

## Disk Defragmenter, [790](#)

## disk geometry, [242](#)–245

## disk maintenance utilities, [786](#)–792. *See also specific utilities*

## Disk Management utility, [247](#), [786](#)–788, [793](#)–799

## Disk tab, Windows Resource Monitor, [767](#)–768

## Disk Utility, Mac OS, [551](#)

## `diskpart.exe` utility, [247](#), [684](#)–685, [786](#)–788

dism, exe command, [685](#)–686

DisplayPort, [306](#)

## displays

- analog versus digital, [355](#)
- brightness/lumens, [355](#)
- color depth, [355](#), [584](#)
- configuring, [356](#)–357
- contrast ratio, [355](#)
- CRT, [353](#)
- external monitor, [445](#)
- features of, [355](#)–356
- fluorescent versus LED backlighting, [354](#)
- LCD, [353](#)
- LED, [353](#)–354
- multiple, [356](#)–357, [915](#)
- native resolution, [355](#)
- OLED, [353](#)–354
- overview, [84](#)–86, [362](#)
- plasma, [354](#)
- preventive maintenance, [481](#)–482
- privacy/antiglare filters, [355](#)
- projector, [365](#)
- refresh rate, [355](#), [584](#)
- resolution, [355](#), [583](#)–584
- rotating/removable screens, [433](#)
- settings, [583](#)–584
- troubleshooting, [357](#)–359, [505](#)–506
- types of, [353](#)–354
- Windows systems requirements, [525](#)

- distorted image, [358](#)
- distributed administration, [953](#)
- distributions, Linux, [533](#)
- DivX format, [408](#)
- DLLs (Dynamic Link Libraries), [642](#), [807](#), [910](#), [911](#)
- DLP (Data Loss Protection), [1177](#)
- DMA modes, [250](#)
- DMZ (demilitarized zone), [1011](#)–1012, [1020](#), [1217](#)
- DNAT (Destination Network Address Translation), [1021](#)
- DNS (Domain Name System), [1058](#)–1059, [1063](#), [1064](#), [1125](#)–1126, [1248](#)
- DNS server, [955](#)
- DNSSEC (DNS Security Extensions), [1177](#)
- Do Loop command, [846](#)–847
- Do While loop, [857](#)
- .doc file, [641](#)
- Dock, [550](#)
- docking stations, [305](#), [438](#)
- document files, [641](#)
- document templates, [641](#)
- documentation
  - of changes, [44](#)
  - incident, [38](#)
  - resources, [38](#)–40
  - service, [39](#)
- .docx file, [641](#)
- domain, [616](#), [1085](#)
- domain controller, [1160](#), [1213](#)

- domain names, [1125](#)–1127
- dongles, [437](#)
- DoS (denial of service) attack, [1150](#)
- dot dot attack, [1240](#)
- .dot file, [641](#)
- dot matrix printers, [374](#)–375, [390](#)
- dot pitch, [353](#)
- .dotx file, [641](#)
- double variable type, [854](#)
- double-sided memory, [194](#)
- draft-quality printers, [375](#)
- DRAM (dynamic RAM)
  - DDR, [186](#)
  - DDR2, [186](#)–187
  - DDR3, [188](#)
  - DDR4, [188](#)
  - overview, [182](#)–183
  - rambus, [185](#)–186
  - synchronous, [185](#)
  - types of, [184](#)–187
- dress, proper, [47](#)
- drill/hammer, [1168](#)
- drive activity light, [94](#)
- drive imaging, [611](#)
- drive lock, [1157](#)
- driverquery.exe command., [808](#)

## drivers

- configuring, 090
- dependency, [910](#)
- failure, [720](#)–721
- incompatibility, [910](#)
- keyboard, [329](#)
- loading, [706](#)–711
- overview, [705](#)
- permissions to install, [719](#)
- Plug and Play, [715](#)–718
- Prep Test, [723](#)–724
- problems with, [909](#)–910
- removing, [713](#)–714
- signed and unsigned, [714](#)–715
- third-party, [620](#)
- updating, [473](#), [713](#), [944](#)
- verifying installation, [720](#)
- versions of, 090

DRM (Digital Rights Management), [1184](#)

Dropbox, [931](#)

drum scanner, [402](#)

DSL (Digital Subscriber Line), [1129](#)

DSL modem, [987](#), [1137](#)

DSN (Data Source Name), [820](#)

DTC (Distributed Transaction Coordinator), [810](#)

DTDs (Document Type Definitions), [1115](#)

dual-core processor, [143](#)–144

- dual-scan, [428](#)
- dump file, [757](#)
- dumpster diving, [1156](#)–1157
- duplexing, [376](#)
- Duron processor (AMD), [164](#)
- dust, [64](#), [478](#)
- DV format, [408](#)
- DVD drives, [77](#), [484](#)
- DVD-A connector, [306](#)
- DVD-ROM drive, [442](#)
- DVDs (digital versatile discs)
  - bootable, [222](#), [610](#)
  - overview, [270](#)–271
  - standards, [271](#)
  - transfer rates, [270](#)
  - troubleshooting, [484](#)
- DVI (Digital Visual Interface), [349](#)
- DVI-D connector, [306](#)
- DVI-I connector, [306](#)
- dxdiag.exe (DirectX Diagnostic Tool), [817](#)
- dynamic disk, [617](#), [787](#)

## ***E***

- E1000e, [593](#)
- Ease of Access Center, [576](#)
- Easy Transfer, [589](#), [627](#)
- eavesdropping attack, [1151](#)



- ECC (error-checking) memory, [191](#)
- echo command, [847](#)
- EDB (Execute Disable Bit), [145](#)
- EDGE (Enhanced Data for GSM Evolution), [1131](#)
- EEPROM (electrically erasable programmable ROM), [101](#), [181](#)
- EFS (Encrypting File System), [1173](#), [1223](#)–1224
- EGA (Enhanced Graphics Adapter), [304](#), [347](#)
- EIDE (Enhanced Integrated Drive Electronics), [115](#), [248](#), [317](#)
- EIDE controllers, [116](#)
- 802.11 wireless networking standards, [1004](#)–1007
- EISA slot, [122](#)
- elasticity, cloud, [595](#)–596
- electrical fire safety, [61](#), [64](#)
- electromagnetic destruction, [1168](#)
- electromagnetic interference (EMI), [478](#)–479
- electrostatic discharge (ESD), [477](#)–478
- email
  - connectivity issues, [990](#)
  - decryption, [459](#)
  - filtering, [1177](#)
  - hijacked, [1245](#)
  - missing settings, [459](#)
  - protocols, [1109](#)–1113
  - scanning, [1235](#)
  - spoofing, [1150](#)
- embedded systems, [956](#)

## Emergency Repair Process

- factory repair partition, [928](#)

- overview, [927](#)–928

- Startup Repair, [928](#)

- System Image Recovery, [931](#)

EMI (electromagnetic interference), [60](#)–61, [971](#)

eMMC (embedded MultiMediaCard), [272](#)

emulation, [593](#)–594

Encapsulated PostScript files, [643](#)

enclosures, [68](#)

encoding, [1109](#)

encryption

- best practices, [1180](#), [1223](#)–1224

- BitLocker, [1173](#), [1224](#)

- BitLocker-To-Go, [1224](#)

- drive, [225](#)–226

- EFS, [1173](#), [1223](#)–1224

- enabling, [1226](#)

- mobile devices, [1182](#)

- overview, [1166](#), [1173](#)

- wireless network, [1017](#)–1018, [1019](#), [1138](#)

Encrypt attribute, [649](#)–650

End Process Tree, [766](#)

end user education, [1248](#), [1249](#)

end-of-life, [553](#)

end-point management server, [956](#)

end-user acceptance, [43](#)

- end-user device configuration, [1136](#)
- Energy Star, [283](#)
- enhanced keyboard, [329](#)
- Enlightenment, [533](#)
- enterprise license, [1185](#)
- entry control roster, [1163](#)
- environment variables, [835](#)
- environmental controls, [64](#), [473](#)–480
- EPA (Environmental Protection Agency), [65](#)
- EPROM (erasable programmable ROM), [79](#), [181](#)
- EPS connector, [290](#)
- .eps file, [643](#)
- equipment grounding, [60](#)
- `erase` command, [677](#)
- e-readers, [451](#)–452
- ergonomic keyboard, [329](#)–330
- ergonomics, [69](#)–70
- error messages, [492](#)
- Error Reporting Tool, [889](#)–890

errors. *See also* [disaster recovery](#); [troubleshooting](#)

auto-restart, [900](#)–902

blue screen, [902](#)–905

boot process, [877](#)–884

compatibility, [912](#)–913

device driver and service, [909](#)–910

device-related, [885](#)–887

diagnostic tools, [889](#)–891

failure to start GUI, [888](#)

overview, [877](#)

paging file, [887](#)

Prep Test, [893](#)–895

eSATA (External SATA), [78](#), [117](#), [130](#), [266](#)–267, [319](#)

escalation, [36](#)

ESD (electrostatic discharge), [58](#)–60, [63](#)

ESD mats, [59](#)

ESSID (Extended Service Set Identifier), [1002](#)

Ethernet, [377](#), [973](#)

EULA (End User Licensing Agreement), [1185](#)

EV-DO (Evolution-Data Optimized, or Evolution-Data Only), [1131](#)

Event Viewer, [589](#), [812](#)–814, [890](#)–891, [910](#), [1247](#)

## exams

- adaptive, [23](#)
- arriving at location, [25](#)–26
- book as preparation tool, [1](#), [2](#), [24](#)–25
- cost of, [25](#)
- Exam 220-1001, [23](#)–24, [1253](#)–1261
- Exam 220-1002, [23](#)–24, [1262](#)–1269
- objectives, [22](#)–23
- online practice, [6](#)
- overview, [21](#)–22
- pass level, [28](#)
- retake policy, [28](#)
- scheduling, [25](#)
- taking, [26](#)–28
- tips for, [25](#)–27

Excel documents, [641](#)

executable files, [638](#)–644

Executive Services, [566](#)

exFAT, [570](#), [617](#)–618

exit rollers, [370](#)

expansion cards, [129](#)–130

expansion slots, [103](#), [124](#), [129](#)–130

expectations, [48](#)

Explorer, [823](#)

ExpressCards, [418](#), [438](#)–439

ext3/ext4 file systems, [618](#)

extended attributes, [647](#)–655

extended partition, [786](#)  
extenders, [980](#)–981  
external cache, [97](#)  
external cloud, [599](#)  
external hard drives, [274](#), [441](#), [442](#)  
external monitor, [445](#)  
external ventilation, [474](#)  
eyes, [69](#)

## *F*

factory recovery partition, [620](#)  
factory repair partition, [928](#)  
failed attempts lockout, [1179](#)  
fanless/passive cooling, [170](#)  
fans  
    auto-restart issues, causing, [900](#)  
    overview, [81](#)  
    power connectors, [114](#)  
    printers, [486](#)  
    speed, [232](#)  
Fast SCSI-2, [262](#)  
Fast Wide SCSI-2, [262](#)  
FAT (Fat Allocation Table), [569](#)–570, [617](#)–618, [685](#), [791](#)  
FAT32, [569](#)–570, [617](#)–618  
F-connector, [966](#)  
Fedora, [533](#)  
feeder, [376](#)

- feeder, printer, [376](#)
- female port, [105](#)
- fiber connection, [1130](#)
- fiber local connector, [970](#)
- fiber optic cables, [969](#)–970
- File and Printer Sharing, [1074](#)–1075
- file associations, [635](#)–638
- file attributes, [645](#)–647
- File DSN, [820](#)
- File Explorer, [823](#)
- file extensions, [638](#)–644
- File History, [932](#)–933
- file recovery software, [247](#)
- file server, [955](#)
- file systems, [569](#)–570, [617](#)–618
- file-naming conventions
  - file associations, [635](#)–638
  - file extensions, [638](#)–644
  - length, [633](#)–634
  - overview, [632](#)–633
  - Prep Test, [660](#)–662

## files

attributes, [683](#)

backing up, [34](#)–35

compressed, [647](#)–649

copying and moving, [673](#)–677, [1209](#)–1210

cross-linked, [792](#)

disappearing, [1245](#)

encrypted, [649](#)–651

fragmented, [678](#), [788](#)

indexed, [652](#)–654

Linux, [1138](#)

missing, [911](#)

offline, [586](#)

Program, [585](#)–586

renaming, [677](#)

shared, [1210](#)–1212

swap, [696](#)

system, [585](#), [641](#), [1212](#), [1245](#)

temporary, [585](#), [773](#)–774

user, [584](#)–585, [627](#)

FilterKeys, [331](#)–332

Finder, [548](#)

fingerprint reader, [1159](#)–1160



## firewalls

- best practices, [1222](#)
- demilitarized zone, [1217](#)
- hardware, [1218](#)
- mobile devices, [461](#)
- overview, [986](#), [1215](#)–1216
- port security and exceptions, [1218](#)–1219
- settings, [1020](#), [1089](#)–1090, [1137](#)–1138
- software, [1218](#), [1248](#)
- SOHO, [1134](#), [1135](#), [1138](#)–1139
- Windows, with Advanced Security, [1219](#)–1221

## FireWire (IEEE 1394)

- ports, [110](#)–111
- printers, [380](#)
- versions of, [110](#)–111

## FireWire cards, [338](#)

## firmware

- defined, [181](#)
- keyboard, [329](#)
- overview, [81](#)–82
- printer, upgrading, [381](#)
- SOHO, [1136](#)
- updating, [212](#), [473](#), [944](#)
- wireless network components, [1012](#), [1020](#)

## first response, [1183](#)

## 5G, [1024](#), [1131](#)

## fixed focus camera, [406](#)

- flash drives, [77](#), [272](#)
- flash memory, [439](#), [456](#)
- flash RAM, [79](#)
- flash ROM, [212](#)
- flash storage cards, [340](#)
- flashing, [212](#)
- flatbed scanners, [402](#)
- FlexATX motherboard, [123](#)
- flickering image, [358](#)
- floppy disk drive, [218](#), [289](#)–290, [692](#)
- flow control, [507](#)
- fluorescent backlit displays, [354](#)
- Folder Lock, [1173](#)
- folders
  - redirection, [1193](#)
  - shared, [1075](#)–1078
  - system, [1212](#)
- Folders Explorer Bar, [575](#)
- fonts, [576](#), [585](#)
- For Each Next loop, [844](#)–845
- For loop, [858](#), [864](#)–865, [867](#), [870](#)
- For Next loop, [845](#)
- Force Quit, Mac OS, [551](#)
- ForEach loop, [858](#)
- form factors
  - defined, [84](#)
  - motherboard, [119](#)–123

`format.com` utility, [247](#), [685](#)  
formatting hard drive, [1169](#)  
4:3 aspect ratio, [348](#)  
4G, [1024](#), [1131](#)  
F-PROT, [1234](#)  
FQDN (fully qualified domain name), [1057](#)–1058  
fragmented files, [678](#), [788](#)  
FreeBSD, [534](#)  
friction feeders, [368](#)  
front panel, [94](#), [108](#)  
FSB (front side bus), [159](#)  
FTP (File Transfer Protocol), [1062](#), [1105](#), [1117](#)–1118  
full backups, [1171](#)  
Full Control permission, [1207](#)  
full name, user account, [1196](#)  
full-duplex, [987](#), [1090](#)  
function keys, [328](#), [432](#)–433, [445](#)  
functionality, verifying, [37](#)  
functions, VBScript, [843](#)–844  
fuser rollers, [370](#)

## G

gadgets, [527](#)  
game pads, [340](#)  
gaming system, [555](#)  
garbled characters, when printing, [388](#)  
gateways, [982](#)–983

GDPR (General Data Protection Regulations), [1185](#)

General tab, [776](#)

geotracking, [453](#)

gestures, [549](#)

get-Command, [851](#)

ghost cursor, [447](#)

.gif file, [643](#)

Gigabit Ethernet standards, [974](#)–975

gigahertz, [138](#)

Gmail, [602](#)

GNOME, [533](#)

GNU/Linux, [533](#)

Google

Apps, [458](#), [602](#)

Authenticator, [454](#)

Drive, [457](#)

Play, [453](#), [461](#)

Gopher, [1114](#)

goto statement, [835](#)

GParted, [941](#), [941](#)–942

GPO (Group Policy Objects), [681](#)–683

gpreresult command, [681](#)–683

GPS (global positioning system), [453](#), [455](#), [460](#)

GPT (GUID Partition Table), [786](#)–787

GPU (graphics processing unit), [85](#), [145](#), [184](#)

gpupdate command, [681](#)–682

graphic files, [643](#)

- Graphic Interchange Format, [643](#)
- graphics accelerator cards, [350](#)
- graphics/CAD/CAM workstation, [555](#)
- grayware, [1155](#)
- grep command, [540](#)–541
- grey-hat hackers, [1146](#)
- ground connectors, [479](#)
- grounding strap, [60](#)
- group policies, [1193](#)
- groups, [1198](#)–1201
- GRUB, [883](#)–884
- guest accounts, [1179](#), [1196](#)
- GUI (graphical user interface)
  - enhancements, optimization of, [778](#)–780
  - failure to start, [888](#)
  - Linux OS, [535](#)–536, [884](#)
  - macOS, [548](#), [549](#)
  - overview, [519](#)–520
  - Windows, [526](#)–532, [657](#)–658
- GUID (globally unique identifier), [226](#)–227

## **H**

- hackers, [1146](#)
- Hacking for Dummies (Beaver), [1147](#)
- hal.dll file, [882](#)–883
- half-duplex, [987](#), [1090](#)
- handheld devices. *See* [mobile devices](#)

handheld scanner, [402](#)

handles, [752](#)

hard drive cables

IDE, [317](#)–318

SATA, [318](#)–319

SCSI, [319](#)–320

hard drive controller, [248](#)

## hard drives

- adding, [797](#)
- assigning/changing drive letters, [793](#)–794
- bottlenecks, [750](#)
- cables, [317](#)–320
- CMOS setup program settings, [216](#)–218
- defragmentation, [788](#)–790
- destruction of, [1168](#)–1169
- disk geometry, [242](#)–245
- disk maintenance utilities, [786](#)–792
- encryption, [225](#)–226
- external, [274](#), [441](#), [442](#)
- formatting, [1169](#)
- initializing, [794](#)
- laptop, [419](#), [441](#)
- mounting, [794](#)
- optimizing, [772](#)
- overview, [77](#)
- platters, [242](#)–243
- power connectors, [78](#), [114](#)–118
- Prep Test, [277](#)–279
- preventive maintenance, [483](#)–484
- printer, upgrading, [381](#)
- RAID, [1172](#)–1173
- recycling, [1168](#)
- sanitation/drive wipe/overwrite, [1169](#)–1170
- status, [793](#)

terminology, [241](#)–247

troubleshooting, [275](#)–276, [500](#)–502

Windows systems requirements, [525](#)

hardening system, [1221](#)

hardware

address, [979](#)

defined, [81](#)–82

firewalls, [1218](#)

print server, [380](#)

requirements, [615](#)

tokens, [1162](#)

tools, [56](#)–57

hashtable variable type, [854](#)

HBA (host bus adapter), [508](#)

HD DB-15 connector, [304](#)

HD-15 connector, [304](#)

HDMI (High-Definition Multimedia Interface), [305](#), [349](#)

head positioning mechanism, [243](#)

headphones, [360](#)

heat pipes, [170](#)

heat sinks, [81](#), [171](#)–172

heating element, printer, [376](#)

help command, [687](#)

hertz, [138](#)

HFS (Hierarchical File System), [618](#)

HGC (Hercules Graphics Card), [304](#)

hibernate mode, [425](#)–426, [579](#)



- Hidden attribute, [646](#)–647, [656](#)
- hidden shares, [1079](#)
- High Data Rate (HDR), [1131](#)
- high-level format, [1169](#)
- high-voltage equipment, [62](#)
- hijacked email, [1245](#)
- HIPAA (Health Insurance Portability and Accountability Act), [1174](#)
- HKEY\_CLASSES\_ROOT subtree, Registry, [801](#)
- HKEY\_CURRENT\_CONFIG subtree, Registry, [801](#)
- HKEY\_CURRENT\_USER subtree, Registry, [572](#), [801](#)–803
- HKEY\_LOCAL\_MACHINE subtree, Registry, [572](#), [801](#)–803
- HKEY\_USERS subtree, [801](#)
- hoaxes, [1239](#)–1240
- home folder, [1194](#)
- home routers, [1133](#)–1134, [1138](#)–1139
- home server PCs, [556](#)–557
- home theater systems, [556](#)
- homegroup, [1086](#)–1088
- HomeGroup feature, [579](#)
- host adapter, SCSI, [256](#)–258
- host ID, [1041](#)–1042
- host system, [231](#)
- HOSTS file, [1059](#)–1060
- hot fixes, [565](#)
- hot swapping, [332](#), [717](#)
- .hqx file, [642](#)
- HTC Sense, [456](#)

HTML (HyperText Markup Language), [644](#), [1114](#)–1116  
HTTP (HyperText Transfer Protocol), [644](#), [1063](#), [1105](#), [1113](#)–1114, [1127](#)  
HTTPS, [1063](#), [1116](#)–1117  
hub device, [110](#)  
hubs, [983](#), [1224](#)–1225  
HUD (heads-up display), [412](#)  
humidifiers, [60](#)  
humidity, [67](#), [477](#)  
Hybrid Cloud, [600](#)  
hybrid drives, [77](#), [272](#)  
hybrid topology, [960](#)  
Hypercard, [1113](#)  
hyperthreading, [142](#)–143  
Hyper-V, [144](#), [144](#)–145  
hypervisor, [231](#), [593](#)  
hypothesis evaluation/generation, [28](#)

## *I*

IaaS (Infrastructure as a Service), [599](#)–600  
IAB (Internet Architecture Board), [1104](#)  
IANA (Internet Assigned Numbers Authority), [1127](#)  
ICANN (Internet Corporation for Assigned Names and Numbers), [1127](#)  
IceWM, [533](#)  
iCloud, [455](#), [549](#)  
icons, explained, [2](#), [5](#)  
ID badges, [1162](#)

IDE (Integrated Drive Electronics), [78](#), [115](#)

- ATAPI specification, [249](#)

- cables, [317](#)–318

- drive performance, [250](#)

- EIDE/ATA-2 standard, [249](#)

- IDE/ATA standard, [249](#)

- installing devices, [250](#)–255

- overview, [247](#)–248

IDE compatibility mode, [232](#)

IDS (Intrusion Detection System), [956](#)

IEEE (Institute of Electrical and Electronics Engineers) standards, [975](#)–976

if statement, [834](#)–835, [856](#)

ifconfig command, [542](#)

IIS (Internet Information Services), [1237](#)

Image Recovery, Mac OS, [550](#)–551

image sticking, [505](#)

ImageX, [613](#)–614

IMAP (Internet Message Access Protocol), [1063](#), [1110](#)–1111, [1111](#)

IMEI (International Mobile Equipment Identity), [437](#)

impact printers, [374](#)

impacts, [34](#)

improper shutdowns, [907](#)–909, [926](#)–927

IMSI (International Mobile Subscriber Identity), [437](#)

incident documentation, [38](#)

incident response

- corporate policies, [1186](#)

- documentation, [1183](#)–1184

- first response, [1183](#)

- licensing, [1184](#)–1185

- overview, [1182](#)–1183

- regulated data, [1185](#)

- tracking of evidence/chain of custody, [1184](#)

incineration, [1168](#)

incorrect boot device, [878](#)–879

incorrect colors, monitor, [503](#), [505](#)

incremental backups, [1172](#)

Index attribute, [652](#)–655

indexing, [780](#)–781

indicator lights, [496](#)

INF files, [706](#)

infected systems, recovering, [1244](#)–1246, [1248](#)–1249

infrared (IR) technology

- laptops, [436](#)

- overview, [1000](#), [1022](#)–1023

- ports, [989](#)

- printers, [378](#)–379

infrastructure changes, identifying, [32](#)

infrastructure mode, [386](#), [1001](#)–1002

INI file, [571](#)

.ini file, [642](#)

Initialization files, [642](#)

inkjet printers, [373](#)–374, [390](#)–391

inline UPS, [296](#)

input devices

- keyboard, [327](#)–332

- laptop, [431](#)–435

- mouse, [333](#)–334

- network adapters/cards, [334](#)–337

- other types of, [338](#)–341

- Prep Test, [342](#)–343

input supply voltage, [284](#)

input/output (I/O) devices, [84](#)–86

input-under voltage, [283](#)

installations, Windows

attended installations, [620](#)–621, [620](#)–622

bootable DVD, [610](#)

computer name, [615](#)–616

drive imaging, [611](#)–614

file systems in, [617](#)–618

methods, [609](#)–614

network, [611](#), [620](#)

non-Windows file systems, [618](#)–620

partitions in, [616](#)–617

preparing for, [614](#)–620

troubleshooting, [623](#)–624

unattended, [620](#)–621, [622](#)–623

USB and PXE, [610](#)–611

verifying, [623](#)–624

workgroup/domain in, [616](#)

`install.exe`, [726](#)

instruction pipeline, [153](#), [155](#)

int variable type, [854](#)

integrated cache, [97](#)

## Intel processors

Celeron, [157](#)

Intel Atom, [161](#)

Intel Core 2, [161](#)

Intel Core i3/i5/i7, [95](#), [162](#)

Itanium/Itanium II, [160](#)

overview, [152](#)

Pentium, [153](#)–154

Pentium 4, [95](#), [159](#)–160

Pentium II, [156](#)

Pentium III, [157](#)–158

Pentium M, [161](#)

Pentium Pro, [155](#)–156

Xeon, [158](#)–159

Intel Turbo Boost Technology, [162](#)

Intel VT (Intel Virtualization Technology), [144](#), [231](#)

interference, [447](#)

internal cloud, [599](#)

internal ventilation, [474](#)–477

## Internet

- access methods, [1125](#)
- ASPs, [1107](#)
- browsers, [1120](#)–1124
- browsing, [1124](#)–1127
- cable, [1128](#)–1129
- cellular networks, [1131](#)
- connection types, [1128](#)–1133
- connectivity issues, [1245](#)
- dial-up, [1128](#)
- domain names and websites, [1125](#)–1127
- DSL, [1129](#)
- fiber, [1130](#)
- firewalls, [1138](#)–1139
- home routers, [1138](#)–1139
- ISDN, [1129](#)
- ISPs, [1106](#)–1107
- line-of-sight wireless Internet service, [1131](#)
- mobile hotspots, [1131](#)
- overview, [1103](#)–1104
- satellite, [1130](#)
- T1/T3, [1130](#)
- tethering, [1132](#)
- WiMax, [1133](#)
- wireless, [1130](#)–1131

Internet appliances, [956](#), [986](#)

Internet Connection Sharing, [775](#)



## Internet Explorer

- advanced settings, [1124](#)
- connections settings, [1123](#)
- content settings, [1122](#)
- general settings, [1121](#)
- overview, [1120](#)
- privacy settings, [1121](#)–1122
- programs settings, [1124](#)
- security settings, [1121](#)

## Internet Options, [577](#)

Internet protocols. *See also* [TCP/IP \(Transmission Control Protocol/Internet Protocol\)](#).

- connection types, [1106](#), [1107](#)
- email, [1109](#)–1113
- FTP, [1117](#)–1118
- HTML, [1114](#)–1116
- HTTP, [1113](#)–1114
- HTTPS, [1116](#)–1117
- overview, [1107](#)–1108
- Prep Test, [1140](#)–1142
- SSL, [1116](#)–1117

## Internet resources, [40](#), [990](#)

- intrusion detection, [232](#), [1157](#), [1192](#)
- invalid certificate, [1246](#)
- inventory management, [39](#)
- I/O devices, [362](#)
- iOS, [443](#), [453](#)

IoT (Internet of Things), [1137](#)

IP (Internet Protocol) address

alternate, [1048](#)–1049

host ID, [1041](#)–1042

IPv4 versus IPv6, [1052](#)

network ID, [1041](#)–1042

overview, [1041](#)

private, [1050](#)

SOHO, [1136](#)

static, [1020](#)

IP conflict, [991](#)

IP spoofing, [1150](#)

`ipconfig` (IP configuration) utility, [1065](#)–1066

IPCop, [1138](#)

IPS (In-Plane Switching) displays, [354](#)

IPS (Intrusion Prevention System), [956](#)

IPSec (IP Security), [1011](#), [1167](#)

IrDA (Infrared Data Association), [1000](#)

IRQs (interrupt requests), [233](#)

ISA (Industry Standard Architecture) cards, [233](#)

ISDN (Integrated Services Digital Network), [1129](#)

ISPs (Internet service providers), [1106](#)–1107

Itanium/Itanium II, [160](#)

ITL (Information Technology Infrastructure Library), [38](#)

ITSM (IT Service Management), [38](#)

iTunes, [453](#), [458](#)

`iwconfig` command, [542](#)

## *J*

### JavaScript

- comment syntax symbol, [871](#)
- decision structures, [869](#)–870
- file, [830](#)
- loops, [870](#)
- overview, [868](#)
- variables, [868](#)–869

### Jave Server Page files, [644](#)

### jewelry, [61](#)

### joysticks, [340](#)

### JPEG (Joint Photographic Experts Group), [643](#)

### .jsp file, [644](#)

### jumpers, [118](#)–119, [214](#), [259](#)

## *K*

### K6 processor (AMD), [163](#)

### K6-2 processor (AMD), [163](#)

### K6-III processor (AMD), [163](#)

### KDE, [533](#)

### kernel memory, [753](#)

### kernel mode, [566](#)

### kernel panic message, [905](#)–906

### key fobs, [1162](#)

## keyboard

- accessibility features, [330](#)–332
- capacitive, [329](#)
- configuring, [330](#)–332
- device driver, [329](#)
- enhanced, [329](#)
- ergonomics, [69](#)
- firmware, [329](#)
- groupings on, [328](#)
- installing, [330](#)
- laptop, [419](#), [431](#)–433
- natural or ergonomic, [329](#)–330
- overview, [327](#)
- ports, [86](#)
- ports for, [106](#)–107
- preventive maintenance, [482](#)–483
- PS/2 connector, [330](#)
- replacing, [447](#)
- switch-based, [328](#)
- troubleshooting, [502](#)–503
- USB connector, [330](#)
- Windows, [329](#)

keyboard controller, [99](#)

Keychain, macOS, [548](#)

keycode, [328](#)

keylogger, [1238](#)–1239

keyswitch, [328](#)

kill command, [543](#)

Knoppix, [533](#)

knowledge base, searchable, [38](#)

KVM switch, [340](#)

## *L*

L1 (level 1) cache, [97](#)–[98](#), [141](#), [195](#)

L2 (level 2) cache, [97](#)–[98](#), [141](#), [195](#)–[196](#)

L3 (level 3) cache, [97](#)–[98](#), [141](#), [196](#)

LAN (local area network), [956](#)

LANGuard, [1243](#)–[1244](#)

laplink cable, [989](#)

Laplink PCmover Express, [627](#)

laptops. *See also* [computers](#)

AC adapters, [294](#), [418](#), [426](#)–427

batteries, [418](#), [420](#)–422

communication components, [435](#)–438

components of, [418](#)–420

convertible, [433](#)

disassembling and reassembling, [448](#)–449

docking stations, [438](#)

expanding capabilities of, [438](#)–439

hard drives, [419](#), [441](#)

input devices, [431](#)–435

LCD panels, [428](#)–430

memory, [199](#), [418](#), [439](#)–440

versus mobile devices, [456](#)

power-management features, [423](#)–425

Prep Test, [463](#)–465

preventive maintenance, [485](#)–486

troubleshooting, [444](#)–448

upgrading, [439](#)–442

laser printers

- overview, [369](#)

- paper feeder mechanism, [369](#)

- paper transport path, [370](#)

- power supply, [370](#)

- primary corona wire, [370](#)

- printing process, [371](#)–372

- problems, [391](#)

- toner cartridge, [370](#)

Last Known Good Configuration, [923](#)

latency, hard drive, [245](#)

layered troubleshooting, [31](#)

LCD (liquid crystal display)

- active matrix, [428](#)

- color, [428](#)

- connecting to computer, [430](#)

- cut-off switch, [446](#)

- handling, [429](#)

- laptop, [419](#)

- monochrome, [428](#)

- overview, [353](#), [428](#)

- passive matrix, [428](#)

- touch panel displays, [430](#)

LDAP (Lightweight Directory Access Protocol), [1063](#), [1064](#)

LEAF (Linux Embedded Appliance Firewall), [1138](#)

LED (light-emitting diode), [353](#)–354, [429](#)

LED backlight, [354](#)

- legacy devices, [233](#)
- legacy/embedded systems, [956](#)
- Lempel-Ziv compression, [648](#)
- LFX v1.42, [293](#)
- LGA (land grid array) chip, [147](#), [148](#)
- libraries, [527](#)
- licensing, software, [1184](#)–1185
- lifecycle policy, [553](#)
- lifting techniques, [61](#)
- Lightning cable, [308](#)
- Li-ion (lithium-ion) batteries, [420](#)
- LILO, [883](#)–884
- line conditioners, [296](#)
- linear troubleshooting, [31](#)
- line-in, [108](#), [360](#)
- line-of-sight infrared, [379](#), [436](#), [1000](#)
- line-of-sight wireless Internet, [1131](#)
- line-out, [108](#), [360](#)
- Linux Bible* (Negus), [940](#)
- Linux Mint, [533](#)



## Linux OS

- boot issues, [883](#)–884
- commands, [536](#)–546
- distribution, [533](#)
- file fails to open, [914](#)
- file systems, [618](#)
- file-related problems, [913](#)
- firewalls, [1138](#)
- graphical interface, [884](#)
- GUI elements, [535](#)–536
- Knoppix, [940](#)–941
- overview, [532](#)
- system requirements, [534](#)–535
- terminal window, [536](#)
- versions of, [532](#)–534

Linux Terminal command, [884](#)

liquid-based cooling, [170](#)

liquids, [477](#)

Live DVD, [57](#)

LMHOSTS file, [1057](#)–1058

local resources, [990](#)

local security policies, [1202](#)–1203

Local Security Policy, [719](#)

local shares, [1210](#)–1211

locate command, [540](#)

location tracking, [1181](#), [1182](#)

location tracking, unauthorized, [460](#)

- locator applications, [455](#)
- lockdown cable, [1158](#)–1159
- lockout, failed attempt, [1179](#)
- log entries, [492](#)
- log errors, [1246](#)
- Log On tab, [776](#)
- logic bomb, [1155](#)
- logon name. *See* [usernames](#)
- logon time restrictions, [1179](#)
- LoJack, [226](#)
- long variable type, [854](#)
- loopback address, [1049](#)
- loopback plug, [992](#), [1073](#)
- looping, [836](#)–837
- loops
  - Do Until, [857](#)–858
  - Do While, [857](#)
  - For Each Next, [844](#)–845
  - For, [858](#), [864](#)–865, [867](#), [870](#)
  - ForEach, [858](#)
  - For Next, [845](#)
  - While, [845](#), [865](#), [868](#), [870](#)
- low-level format, [1169](#)
- LPX (low profile extended) motherboards, [120](#)
- ls command, [537](#)
- LTE (Long Term Evolution), [1024](#)
- lumens, [355](#)

LVD (Low Voltage Differential), [263](#)

## *M*

M.2 SSDs, [274](#)

MAC (Media Access Control) address

filtering, [1009](#), [1018](#), [1019](#), [1137](#), [1194](#), [1226](#)

overview, [979](#)

spoofing, [1151](#)

## macOS

best practices, [551](#)–552

crash screens, [905](#)–906

Disk Utility, [551](#)

driver updates, [552](#)

Force Quit application, [551](#)

gestures, [549](#)

GUI elements, [548](#)

iCloud, [549](#)

key features, [548](#)–550

Keychain, [548](#)

multiple desktops/mission control, [548](#)

overview, [443](#), [546](#)–547

patching, [552](#)

remote disc, [550](#)

Screen Sharing, [551](#)

Spotlight, [549](#)

system requirements, [547](#)–548

Time Machine, [550](#), [551](#)–552

tools in, [550](#)–551

updating, [552](#)

versions of, [547](#)

macro virus, [1232](#)

macros, [1232](#)–1233

Magic Packet, [426](#)

magnetic drives, [77](#)

maintenance. *See* [preventive maintenance](#)

male port, [105](#)

malware (malicious software)

adware, [1155](#), [1237](#)–1238

botnet, [1239](#)

keylogger, [1238](#)–1239

overview, [1153](#), [1236](#)–1239

Prep Test, [1250](#)–1251

ransomware, [1155](#), [1238](#)

removing, [1248](#)–1249

rootkit, [1239](#)

spyware, [1155](#), [1237](#)–1238

Trojan horses, [1154](#), [1236](#)

virus, [1154](#)

worms, [1237](#)

MAN (metropolitan-area network), [957](#)

man command, [537](#)

managed switches, [984](#)

man-in-the-middle attack, [1152](#)

mantrap, [1156](#)

Marketplace, [453](#)

master/slave configuration, IDE devices, [252](#)–255

match co-processor, [141](#)–142

MBR (Master Boot Record), [229](#), [246](#)–247, [786](#)–787

MBSA (Microsoft Baseline Security Analyzer), [1242](#)–1243

McAfee, [473](#), [1234](#)

md (mkdir) command, [672](#)

MDA (Monochrome Display Adapter), [304](#), [347](#)

MDM (Mobile Device Management), [462](#), [1194](#)

MDRAM (multibank DRAM), [351](#)

measured service, [596](#)

mechanical mouse, [333](#)

media streaming front-end system, [556](#)

megapixels, [405](#)

## memory

- address bus, [139](#)–140
- auto-restart issues, causing, [901](#)–902
- bad, [901](#)–902
- bottlenecks, [750](#)
- buffered versus unbuffered, [194](#)
- cache, [97](#)–98, [141](#)
- CMOS setup program settings, [219](#)
- committed, [753](#)
- compatibility, [199](#)
- connectors for, [198](#)
- CPU-Z, viewing type with, [188](#), [193](#)
- data bus, [138](#)–139
- DDR, [186](#)
- DDR2, [186](#)–187
- DDR3, [188](#)
- DDR4, [188](#)
- DIMMs, [188](#)–189
- DRAM types, [184](#)–187
- dual-channel configuration, [192](#)
- ECC versus non-ECC, [191](#)
- error-checking, [190](#)–191
- installing or upgrading, [197](#)–201
- kernel, [753](#)
- laptop, [418](#), [439](#)–440
- managing, [562](#), [696](#)–699
- multichannel memory architecture, [192](#)–193

- overview, [79](#)
- paged, [567](#)–569, [753](#)
- parity versus nonparity, [190](#)–191, [199](#)
- physical, [752](#)
- Prep Test, [203](#)–207
- printer, upgrading, [380](#)
- purpose of, [180](#)
- RAM, [182](#)–184
- ROM, [181](#)–182
- single-sided versus double-sided, [194](#)
- SODIMMs, [188](#), [200](#)–201, [418](#)
- speed, [198](#)
- system, [180](#)
- troubleshooting, [498](#)–499
- types of, [179](#)–184, [198](#)
- upgrading, [439](#)–440
- usage, [680](#)
- video, [351](#)
- virtual, [562](#), [696](#)–699, [770](#)–772
- Windows systems requirements, [525](#)
- memory controller, [99](#), [141](#)
- memory sticks, [272](#)
- Memory tab, Windows Resource Monitor, [767](#)
- Mendocino, [156](#)
- mesh topology, [959](#)
- Messenger service, [1095](#)
- metered service, cloud, [596](#)



Metro User Interface, [529](#)

Metropolitan Vacuum Cleaner, [472](#)

MFT (Master File Table), [791](#)

MIC-in port, [108](#)

microATX motherboard form factor, [123](#)

microATX power supplies, [285](#)

MicroDIMM (micro dual inline memory module), [190](#)

microphone, [108](#), [340](#), [360](#)

microphone activation, unauthorized, [1182](#)

microphones, [409](#)–410

Micro-SD cards, [274](#)

Microsoft App Store, [443](#)

Microsoft Console settings files, [643](#)

Microsoft Network Monitor, [1151](#), [1152](#)

Microsoft Terminal Services Client (`mstsc.exe`), [823](#)

Microsoft Windows. *See* [Windows operating systems](#)

middleware, [597](#)

MIDI (Musical Instrument Digital Interface), [341](#), [410](#)–411

MIME (Multipurpose Internet Mail Extensions), [1109](#)

Mini-DisplayPort, [306](#)

Mini-HDMI, [305](#)

mini-ITX motherboard, [123](#)

miniPCI, [129](#)

mini-PCIe (mini-PCI Express) cards, [129](#), [440](#)

Mini-SD cards, [273](#)

mirror disk, [267](#)

mirrored volume, [267](#), [795](#), [1173](#)

missing boot files, [879](#)–883

missing files, [911](#)

MJPEG format, [408](#)

MMC (Microsoft Management Console), [579](#)–580, [787](#), [822](#)–823, [898](#)–899

MMF (multi-mode fiber), [969](#)

MMX (MultiMedia eXtensions), [142](#)

## mobile devices

- antivirus, [455](#)
- encryption, [1182](#)
- e-readers, [451](#)–452
- geotracking, [453](#)
- GPS, [453](#)
- versus laptops, [456](#)
- locator applications, [455](#)
- NFC-enabled, [454](#)
- no field-serviceable parts, [456](#)
- operating systems, [442](#)–443, [451](#), [452](#)–454
- overview, [449](#)–451
- passcode locks, [454](#)
- phablets, [451](#)–452
- Prep Test, [463](#)–465
- protective covers, [456](#)
- remote backup applications, [455](#)
- remote wipes, [454](#)–455
- screen calibration, [453](#)
- screen locks, [454](#)
- screen orientation, [453](#)
- securing, [454](#)–456, [460](#)–462
- security, [1182](#)
- smart camera, [452](#)
- storage, [456](#)
- synchronizing data, [457](#)–458
- tethering, [453](#)

touch interface, [456](#)

troubleshooting, [459](#)–460, [1181](#)–1182

wearable tech, [453](#)–454

mobile operating systems

Android, [452](#)

Apple iOS, [452](#)

application source, [453](#)

basic features, [451](#)

integrated, [456](#)

patching/updates, [455](#)

mobile-ITX motherboard, [124](#)

modem, [108](#)–109, [436](#), [986](#), [987](#)

modem cards, [337](#)

monitoring, [231](#)–232

monitoring tools

overview, [750](#)

Performance Monitor, [758](#)–765

Task Manager, [750](#)–758

Windows Resource Monitor, [765](#)–768

monitors. *See* [displays](#)

Mosaic browser, [1114](#)

## motherboards

ATX, [121](#)–122

BIOS chip, [100](#)–101, [102](#)

chipset, [99](#)–100

CMOS battery, [101](#)–102

CPU sockets, [95](#)

expansion slots, [103](#), [124](#)

FireWire (IEEE 1394) port, [110](#)–111

FlexATX, [123](#)

form factors, [119](#)–123

front panel connector, [108](#)

internal USB connectors, [109](#)–110

ITX, [123](#)–124

LPX (low profile extended), [120](#)

microATX, [123](#)

modem, [108](#)–109

network card, [108](#)–109

NLX (new low profile extended), [120](#)–121

overview, [80](#), [93](#)

performance considerations, [130](#)

power connectors, [112](#)–114

Prep Test, [132](#)–136

RAM slots, [95](#)–96

serial ports, [104](#)–105

sound connector, [108](#)

troubleshooting, [498](#)

USB ports, [109](#)–110

- video adapters port, [106](#)
- motion sensor, [341](#)
- mouse
  - ergonomics, [69](#)
  - installing, [334](#)
  - mechanical, [333](#)
  - optical, [333](#)
  - opto-mechanical, [333](#)
  - ports for, [86](#), [106](#)–107
  - preventive maintenance, [482](#)–483
  - PS/2, [334](#)
  - troubleshooting, [502](#)–503
  - types of, [333](#)–334
  - USB, [334](#)
  - wireless, [333](#)
- move command, [677](#)
- MPEG1 format, [408](#)
- MPEG2 format, [409](#)
- MPEG4 format, [409](#)
- MRTG, [484](#)
- .msc file, [643](#)
- msconfig.exe (System Configuration), [799](#)–801, [889](#)
- MS-DOS, [739](#)–742
- MS-DOS command file, [640](#)
- MSDS (Material Safety Data Sheet), [66](#)
- MsgBox, [847](#)–850
- MSI files, [728](#)

`msinfo32.exe` (System Information tool), [564](#), [811](#)–812

MSRT (Malicious Software Removal Tool), [1242](#)

`mstsc.exe` (Microsoft Terminal Services Client), [823](#)

MTBF (Mean Time Before Failure), [480](#)

MT-RJ (mechanical transfer-registered jack) connector, [970](#)

multiboot, [620](#)

multichannel memory architecture, [192](#)–193

multicore processor, [142](#)–143

multifactor authentication, [1013](#), [1164](#), [1177](#), [1193](#)

multifunction printers, [374](#)

multimedia cards, [362](#)

multimedia connectors, [307](#)

multimedia devices

- camcorders, [411](#)–412
- digital cameras, [404](#)–406
- digital video cameras, [407](#)
- microphones, [409](#)–410
- MIDI, [410](#)–411
- overview, [401](#)
- Prep Test, [414](#)–415
- QR scanners, [412](#)
- scanners, [401](#)–404
- signature pads, [412](#)
- TV tuners, [411](#)–412
- video capture cards, [411](#)–412
- VR headsets, [412](#)
- web cameras, [407](#)

- multimeter, [57](#), [58](#), [992](#)
- multimonitor taskbars, [530](#)
- multiple branch prediction, [155](#)
- multiple desktops, [532](#), [548](#)
- multiple display, [356](#), [915](#)
- multiple shares, [1079](#)
- multipurpose cables
  - Lightning, [308](#)
  - Thunderbolt, [309](#)
  - USB, [310](#)–312
- multitasking
  - cooperative, [732](#)–733, [738](#)
  - defined, [732](#)
  - preemptive, [732](#)–734
- multithreaded applications, [734](#)
- multitouch, [456](#)
- `mv` command, [538](#)

## N

- name resolution, TCP/IP, [1053](#)–1061
- nano-ITX motherboard, [124](#)
- NAS (network attached storage) devices, [242](#), [986](#)
- NAT (Network Address Translation), [1021](#), [1051](#), [1134](#), [1137](#)
- native resolution, [355](#)
- Navigation Pane, [574](#)–575
- nbtstat (NetBIOS over TCP/IP Statistics) utility, [1067](#)–1068
- `net` command, [686](#)–687, [899](#)



- net localgroup command, [1070](#)
- net use command, [1071](#)
- net user command, [1069](#)–1070, [1070](#)
- net view command, [1070](#)–1071
- NetBEUI (NetBIOS Extended User Interface), [1038](#)
- NetBIOS (Network Basic Input/Output System), [1063](#)
- NetBIOS name, [1054](#)–1057
- NetBIOS name resolution, [1055](#)
- netbooks, [162](#)
- NetBT (NetBIOS over TCP/IP), [1063](#), [1109](#)
- NetBus, [1154](#), [1155](#), [1236](#)
- netdom command, [1071](#)
- netstat command, [1068](#)–1069
- network adapters/cards
  - built-in, [228](#)–229
  - CMOS setup program settings, [228](#)
  - configuring, [335](#)–336, [1136](#)
  - defined, [335](#)
  - drivers, [1032](#)–1036
  - expansion slots, [130](#)
  - installing, [334](#)–335, [1033](#)–1036
  - laptops, [436](#)
  - 100/1000, [335](#)
  - overview, [108](#)–109, [978](#)–979, [988](#)
  - settings/properties, [1090](#)–1091
  - special-purpose, [337](#)–338
- Network and Sharing Center, [577](#)

network architectures, [973](#)–975

network attacks, [902](#)

network client, [1036](#)–1037

network connections, [1034](#)–1036

Network Connections service, [775](#)

network devices

- bridges, [981](#)–982

- cable/DSL modem, [986](#)

- cloud-based network controller, [986](#)

- Ethernet over power, [986](#)

- firewalls, [986](#)

- gateways, [982](#)–983

- hubs, [983](#)

- Internet appliances, [986](#)

- modems, [986](#)

- network attached storage, [986](#)

- network interface card, [980](#)

- overview, [978](#)

- patch panels, [986](#)

- power over Ethernet, [986](#)

- repeater/extender, [980](#)–981

- routers, [982](#)

- switches, [984](#)

- VoiP phones, [986](#)

- wireless access points, [985](#)

network drive, mapping, [1080](#)–1081

network ID, [1041](#)

- network installation, [611](#)
- network interface cards. *See* [network adapters/cards](#)
- network printer, [385](#), [990](#), [1083](#)–1084
- network protocols, [1038](#)–1039
- network resources, browsing, [1081](#)–1082
- network switch, [1134](#)
- Network tab, Windows Resource Monitor, [768](#)
- network topology diagrams, [38](#)
- Network+ certification, [7](#)
- network-attached storage device, [555](#)–556
- network-based attacks, [1148](#)–1153

## networking

access control, [1194](#)

access methods, [971](#)–972

architectures, [973](#)–975

authentication, [1013](#)

bottlenecks, [750](#)

cabling, [962](#)–970

centralized administration, [953](#)

communication methods, [987](#)–988

computers, [988](#)–989

connection, establishing, [1091](#)–1092

distributed administration, [953](#)

network profiles, [1088](#)–1089

overview, [951](#)

planning network components, [1039](#)–1040

Prep Test, [992](#)–998, [1096](#)–1101

protocols, [975](#)–978, [1038](#)–1039

software components, [1031](#)–1040

tools, [991](#)–992

topologies, [957](#)–961

troubleshooting, [989](#)–992, [1071](#)–1073

types of networks, [951](#)–956

with Windows, [1084](#)–1093

Networking tab, Task Manager, [755](#)

NFC (Near Field Communication), [454](#), [1022](#)–1023

NGFF (Next Generation Form Factor), [274](#)

NICs. *See* [network adapters/cards](#)

NiMH (nickel-metal hydride) batteries, [420](#)

NLX (new low profile extended) motherboard, [120](#)–121

NNTP (Network News Transfer Protocol), [1064](#)

No operating system found error, [878](#)

noise, as power issue, [295](#)

non-compliant systems, [1174](#)

non-ECC memory, [191](#)

non-integrated cache, [97](#)

nonparity memory, [190](#)–191, [199](#)

nonunicast traffic, [755](#)

non-Windows file systems, [618](#)–619

North Bridge chip, [99](#)–100

Norton Security, [1234](#), [1236](#)

NoteMaster, [457](#)

Notepad, [823](#)

notification area, [580](#)

NSCA (National Center for Supercomputing Applications), [1114](#)

nslookup utility, [1069](#)–1070

NT (New Technology), [521](#)

ntdetect.com boot file, [880](#)–881

NTFS (New Technology File System), [521](#), [569](#)–570, [617](#)–618, [647](#), [1206](#), [1210](#)

ntldr boot file, [879](#)–880

ntoskrnl.exe command, [693](#)–694, [882](#)–883

ntuser.dat, [886](#)

NTVDM (NT Virtual DOS Machine), [739](#)

null modem cable, [314](#)–315, [989](#)

numeric keypad, [328](#)

NVMe (Non-Volatile Memory Express), [274](#)

## O

object access auditing, [1213](#)

OCP (over-current protection), [283](#), [285](#)

ODBC Data Source Administrator, [819](#)–821

Office 2003 macros, [1232](#)–1233

Office 2016 macros, [1233](#)

Office 365, [602](#)

offline files, [586](#)

off-site email applications, [602](#)

offsite storage, [1172](#)

ohm, [282](#)

Ohm's Law, [282](#)

OLE (Object Linking and Embedding), [807](#)

OLED (organic light-emitting diode), [353](#)–354, [429](#)

OLGA (organic land grid array), [160](#)

on demand service, [595](#)

onboard cache, [229](#), [230](#)

onboard video cards, [129](#)

100 Mbps Ethernet standards, [974](#)

100/1000 network card, [335](#)

100BaseFX, [974](#)

100BaseT, [974](#)

1000BaseLX, [974](#)

1000BaseSX, [974](#)

1000BaseT, [974](#)

OneDrive, [455](#), [530](#), [603](#), [931](#)

online test bank, [6](#)

online UPS, [296](#)

open source license, [1185](#)

OpenBSD, [534](#)

openSUSE, [533](#)

Opera browser, [727](#)

operating systems (OS). *See also specific operating systems*

- choosing an optimal system, [554](#)–557

- compatibility concerns, [554](#)

- difference and similarities, [552](#)–554

- end-of-life, [553](#)

- mobile devices, [442](#)–443, [451](#), [452](#)–454

- overview, [79](#), [519](#)–520

- patching/updates, [455](#)

- Prep Test, [558](#)–559

- 32-bit versus 64-bit, [520](#)

- update failures, [1245](#)

- update limitations, [554](#)

- vendor-specific limitations, [553](#)

Opteron processor (AMD), [164](#)

optical drives

- CMOS setup program settings, [218](#)

- overview, [77](#)

- troubleshooting, [502](#)

optical mouse, [333](#), [483](#)

- optical zoom, [406](#)
- optimization of Windows environment, [774](#)–776
  - best practices, [770](#)–781
  - bottlenecks, areas of, [750](#)
  - GUI enhancements, [778](#)–780
  - hard drive, [772](#)
  - indexing, [780](#)–781
  - overview, [749](#)
  - Performance Monitor, [758](#)–765
  - Prep Test, [782](#)–783
  - printers, [772](#)–773
  - services, [774](#)–778
  - solid-state drive, [772](#)
  - Task Manager, [750](#)–758
  - temporary files, [773](#)–774
  - virtual memory, [770](#)–772
  - Windows Resource Monitor, [765](#)–768
- opto-mechanical mouse, [333](#)
- organizational units, Active Directory, [1193](#)–1194
- OSI (Open Systems Interconnect) model, [977](#)–978
- OTP (One-Time Password) token, [1162](#)
- out of memory error, printer, [391](#)
- out of paper error, printer, [387](#)
- Outlook 2016 client, [1111](#)–1114
- Outlook online, [602](#)



output devices

displays, [78](#), [352](#)–359

overview, [84](#), [345](#)

Prep Test, [364](#)–366

sound card, [359](#)–362

video adapters, [345](#)–352

overclocking, [146](#)

overheat shutdown, display, [358](#)

oversized images/icons, display, [359](#)

## ***P***

P4 connector, [290](#)

PaaS (Platform as a Service), [601](#)

PAC (pin array cartridge), [160](#)

packet sniffers, [1151](#)

packets, [1150](#)–1151

page faults, [756](#)

page file, [567](#)

page printers. *See* [laser printers](#)

paged memory, [753](#)

PageDefrag, [771](#)

paging file, [887](#)

pairing, [437](#), [1021](#)

PAN (personal-area network), [957](#)

paper documents, destroying, [1170](#)

paper feeder mechanism

continuous form feeders, [368](#)

friction feeders, [368](#)

overview, [367](#)–368

paper jams, [387](#), [390](#), [391](#)

paper tray, [376](#)

paperless office, [375](#)

parallel mode, [266](#)

parallel ports, [105](#), [220](#)–221, [989](#)

parallel processing, [154](#)

parent controls, [1021](#)

parity

data, [1173](#)

error, [191](#)

memory, [190](#)–191, [199](#)

serial ports, [507](#)

partitions, hard drive

copying and moving files across, [1209](#)–1210

creating, [794](#)–795

extending, [786](#), [795](#)–796

factory recovery partition, [620](#)

factory repair partition, [928](#)

overview, [616](#)–617

recovery, [938](#)

shrinking, [796](#)

splitting, [796](#)–797

types of, [795](#)

- pass level, exams, [28](#)
- passcode locks, [454](#)
- passive cooling, [170](#)
- passive heat sink, [172](#)
- passive matrix display, [428](#)
- pass-through connector, [508](#)
- `passwd` command, [541](#)–542
- password attacks, [1148](#)–1150
- password policy, [39](#)
- passwords
  - administrator, [223](#)–225
  - best practices, [1178](#)–1179, [1222](#)
  - BIOS/UEFI, [1157](#), [1158](#), [1174](#), [1179](#)
  - default, changing, [1180](#)
  - email, [1111](#)
  - expiration, [1178](#)–1179
  - mobile devices, [1182](#)
  - power-on, [223](#)
  - requirements, [1176](#)
  - routers, [1225](#)
  - SOHO, [1135](#)
  - strong, [1163](#), [1177](#), [1178](#)
  - user, [223](#)–225
  - user accounts, [1196](#)–1197
  - wireless network, [1008](#), [1016](#)–1017, [1019](#)
  - workstation, [1179](#)
- PATA (Parallel ATA), [317](#)

- PATA Emulation mode, [232](#)
- patching, [455](#), [552](#), [1180](#), [1222](#)
- pathping utility, [1069](#)
- PC Paintbrush, [643](#)
- PC Refresh and Reset, [934](#)
- PC repair toolkit, [56](#)
- PC-BSD, [534](#)
- PCI (Payment Card Industry), [1185](#)
- PCI (Peripheral Component Interconnect), [78](#), [84](#), [124](#)–125
- PCIe (Peripheral Component Interconnect Express)
  - 6-pin power connector, [113](#)
  - 8-pin connector, [290](#)
  - expansion slots, [103](#)
  - overview, [84](#), [128](#)
  - PCI Express 1x, [103](#)
  - PCI Express 16x, [103](#)
  - sound cards, [360](#)
- PCI-X (PCI Extended) bus architecture, [127](#)
- PCMCIA (Personal Computer Memory Card Industry Association), [125](#)–126, [438](#)
- .pcx file, [643](#)
- PDF (Portable Document Format), [641](#), [643](#)
- PDU (power distribution unit), [207](#)
- peer servers, [953](#)
- peer-to-peer (P2P) networks, [952](#)–953

- Pentium processors (Intel), [96](#), [150](#)
  - clock multipliers, [153](#), [154](#)
  - Pentium 4, [95](#), [159](#)–160
  - Pentium II, [156](#)
  - Pentium III, [157](#)–158
  - Pentium M, [161](#)
  - Pentium Pro, [155](#)–156
- Performance Logs and Alerts, [775](#)
- Performance Monitor, [758](#)–765
- Performance tab, Task Manager, [751](#)
- peripheral power connector, [290](#)
- permissions
  - allow versus deny, [1208](#)
  - for copying and moving files, [1209](#)–1210
  - defined, [1201](#)
  - directory, [1177](#)
  - inheritance/propagation, [1207](#), [1210](#)
  - NTFS versus share, [1210](#)
  - overview, [1165](#), [1205](#)–1206
  - restricting, [1179](#)
  - shared folder, [1077](#)
- personal computers, [76](#). *See also* [computers](#)
- personal firewall software, [1218](#)
- personal license, [1185](#)
- personal safety, [61](#)–62
- PF (Page File), [751](#)
- PFC (Power Factor Corrected) power supply, [296](#)

PGA (pin grid array) chip, [147](#), [167](#)–168  
phablets, [451](#)–452  
Phenom II processor (AMD), [165](#)  
Phenom processor (AMD), [165](#)  
PHI (Protected Health Information), [1185](#)  
phishing, [1148](#), [1239](#)  
PHP: Hypertext Preprocessor, [644](#)  
physical infrastructure, cloud, [596](#)–597  
physical memory, [752](#)  
physical security, [1156](#), [1175](#)–1176  
pickup rollers, [369](#), [486](#)  
PIF (program information file), [739](#)–742  
PII (Personally Identifiable Information), [1185](#)  
`ping` (Packet Internet Groper) command, [1065](#)–1066  
pinning, [529](#), [589](#)  
PIO (Programmed I/O) mode, [250](#)  
pipe ( | ) command, [541](#)  
pipeline, [852](#), [862](#)  
pixels, [86](#), [505](#)  
PKZIP file, [642](#)  
plasma displays, [354](#), [429](#)  
platters, hard drive, [242](#)–243  
plenum, [971](#)  
Plug and Play, [233](#), [715](#)–718  
PMT (photomultiplier tube), [402](#)  
PNG (Portable Network Graphics), [644](#)  
PnP BIOS (Plug and Play BIOS), [226](#)

PoE (Power over Ethernet), [986](#), [1091](#)

Point and Print feature, [1083](#)–1084

pointing devices. *See also* [mouse](#)

- digitizer, [435](#)

- overview, [433](#)

- pointing stick, [434](#)–435

- stylus, [435](#)

- touch pad, [433](#)–434

- touch stick, [434](#)–435

pointing stick, [434](#)–435

polarity base, [479](#)

POP3 (Post Office Protocol version 3), [1063](#), [1110](#), [1111](#)

pop-ups, [1239](#), [1244](#)

port forwarding, [1137](#)

port replicators, [438](#)

portable computers. *See* [laptops](#)

ports. *See also specific ports*

DB25-female, [105](#)

disabling, [1020](#), [1177](#)

FireWire (IEEE 1394), [110](#)–111

forwarding, [1020](#)

hubs, [110](#)

mapping, [1020](#)

overview, [86](#), [104](#), [303](#)–304

parallel, [105](#), [220](#)

RJ-45, [108](#)–109

security, [1194](#)

security and exceptions, [1218](#)–1219

serial, [104](#), [506](#)–507

TCP/IP, [1062](#)–1063

triggering, [1020](#)

video adapter, [106](#), [107](#)

positive attitude, [46](#)

POST (Power-On Self Test), [79](#), [82](#), [101](#), [181](#), [211](#), [692](#), [906](#)

posture, [69](#), [70](#)

power buttons, [94](#)

power conditioning, [479](#)



power connectors

ATX, [113](#), [287](#)–289

8-pin PCIe connector, [291](#)–292

fans, [113](#)

hard drives, [114](#)–118

motherboard, [112](#)–114

overview, [287](#)

peripheral, [290](#)

SATA, [291](#)

6-pin PCIe connector, [291](#)–292

12-volt, [290](#)–291

power consumption, [286](#), [480](#)

power converters, [281](#)

power level, wireless network, [1015](#)–1016, [1019](#)

power light, [94](#)

power management, laptop

ACPI, [423](#)

APM, [423](#)

configuring, [423](#)–426

hibernate mode, [425](#)–426

standby, sleep, and suspend modes, [423](#)–425

wake on LAN, [426](#)

power plans, Windows, [578](#)

## power supply

- AC adapters, [294](#)

- ATX, [113](#), [284](#)–285, [287](#)–293

- auto-restart issues, causing, [901](#)

- DC adapters, [295](#)

- disconnecting, [61](#)

- form factors, [292](#)–293

- hot-swappable, [293](#)

- identifying, [284](#)–287

- issues in, [295](#)

- microATX, [285](#)

- overview, [80](#), [281](#)

- PFC, [296](#)

- power consumption by product, [286](#)

- power maintenance, [481](#)

- Prep Test, [298](#)–299

- printer, [370](#)

- purpose of, [283](#)–284

- safety tips, [62](#)–63

- specification, [283](#)

- terminology, [282](#)–283

- testing, [510](#)–511

- troubleshooting, [509](#)–513

- UPS, [295](#)–297

- power surges, [67](#), [295](#)

- power users, [1199](#)

- power-on password, [223](#)

PowerPoint documents, [641](#)

PowerShell script

- Boolean operators, [856](#)

- calling script, [851](#)–852

- Cmdlets, [852](#)

- comment syntax symbol, [871](#)

- comparison operators, [855](#)

- decisions, [855](#)–856

- declarations, [853](#)–854

- external commands, [861](#)

- file extension, [640](#)

- functions, [854](#)–855

- If statement, [856](#)

- loops, [857](#)–858

- main procedure, [854](#)–855

- opening and saving files, [860](#)–861

- overview, [531](#), [851](#)

- parameters, [861](#)

- pipeline, [862](#)

- screen output, [859](#)

- script structure, [852](#)–855

- Switch statement, [856](#)–857

PowerShell script file, file extension, [830](#)

- .pps file, [641](#)

- .ppsx file, [641](#)

- .ppt file, [641](#)

- .pptx file, [641](#)

- pre-assessment, [3](#), [9](#)–17
- preemptive multitasking, [732](#)–734
- preinstallation environments, [1247](#)
- preventive maintenance
  - case and components, [480](#)–481
  - drives, [483](#)–484
  - environmental controls, [473](#)–480
  - keyboards and mice, [482](#)–483
  - laptops, [485](#)–486
  - materials and equipment, [472](#)
  - monitor, [481](#)–482
  - power supply, [481](#)
  - Prep Test, [488](#)–489
  - printers, [395](#)–396, [486](#)–487
  - reasons to perform, [470](#)
  - scanners, [486](#)–487
  - scheduling, [471](#), [944](#)
  - software utilities for, [472](#)–473
  - storage media, [483](#)–484
  - tools for, [472](#)–473
- preventive measures, implementing, [37](#)
- primary corona wire, [370](#)
- principle of least privilege, [1178](#), [1194](#)
- print drum, [370](#), [371](#)
- print heads, [376](#), [486](#)
- print jobs tasks, [393](#)
- Print Management console, [385](#)–386

print queue tasks, [393](#)

print server, [955](#)

Print Spooler service, [388](#)–389, [775](#), [1094](#)

printer operators, [1199](#)

printer port. *See* [parallel ports](#)

## printers

- cloud-based, [375](#)–376
- common parts on, [376](#)
- common problems and tools, [392](#)
- configuring, [382](#)–384
- connections, [377](#)–380
- disk drive, adding, [381](#)
- dot matrix, [374](#)–375, [390](#)
- draft-quality, [375](#)
- driver, [383](#)
- error codes, [387](#)
- FireWire, [380](#)
- firmware, upgrading, [381](#)
- hardware print server, [381](#)
- infrared, [379](#)
- inkjet, [373](#)–374, [390](#)–391
- installing, [381](#)–382, [1083](#)–1084
- laser, [369](#)–373, [391](#)
- memory, upgrading, [381](#)
- multifunction, [374](#)
- network, [385](#), [990](#), [1083](#)–1084
- optimizing, [772](#)–773
- overview, [362](#), [367](#)
- paper feeder mechanism, [367](#)–368
- paper jams, [387](#), [390](#), [391](#)
- Prep Test, [397](#)–399
- preventive maintenance, [395](#)–396, [486](#)–487

- print jobs, [393](#)
- safety, [394](#)–395
- SCSI, [380](#)
- sharing, [383](#)–386, [384](#)–386, [1082](#)
- spooling service problems, [388](#)–389, [392](#)
- test page, [383](#), [388](#)
- thermal, [375](#)
- 3D, [376](#)
- troubleshooting, [386](#)–394
- types of, [369](#)–375
- upgrading hardware, [380](#)–381
- USB, [378](#)–379
- virtual, [375](#)–376
- wireless, [378](#)

## privacy

- browser settings, [1121](#)–1122
- privacy filters/privacy screens, [355](#), [1162](#)–1163
- professionalism, [47](#)

private cloud, [598](#)–599

private IP addresses, [1050](#)

privileges, executing, [665](#)–667

PRL (Preferred Roaming List), [438](#)

probable cause, theory of, [33](#)

problems. *See also* [disaster recovery](#); [errors](#); [troubleshooting](#)

- with applications, [910](#)–913

- applications with not install, [911](#)–912

- auto-restart errors, [900](#)–902

- blank screen on boot, [906](#)

- blue screen errors, [902](#)–905

- breaking into smaller pieces, [32](#)

- common, overview of, [897](#)

- compatibility errors, [912](#)–913

- corrupted shortcuts, [910](#)–911

- damaged setting, [911](#)

- device driver and service, [909](#)–910

- device will not function, [915](#)

- device-related, [915](#)

- establishing plan of action for, [36](#)–37

- identifying, [31](#)–32

- improper shutdowns, [907](#)–909

- Linux-related, [913](#)

- missing files or DLLs, [911](#)

- multiple monitor issues, [915](#)

- Prep Test, [916](#)–918

- prioritizing, [32](#)

- prioritizing potential fixes for, [35](#)–36

- proprietary crash screens, [905](#)–906

- requiring or causing reboot, [900](#)–909

- services fail to start, [912](#)

- spontaneous system restart/shutdown, [914](#)



- system lockup, [907](#)–909
- Windows-specific service, [897](#)–899
- procedures, [34](#)
- Processes tab, Task Manager, [755](#)–757
- processing, as basic computer function, [75](#)–76
- processor. *See* [CPU\(central processing unit\)](#).
- professionalism, [44](#), [46](#)–50
- Program files, [585](#)–586
- programs, [726](#). *See also* [applications](#)
- projectors, [354](#)
- proprietary crash screens, [905](#)–906
- protective covers, [455](#)
- proxy server, [955](#), [1051](#)–1052
- ps command, [542](#)
- .ps1 file, [640](#), [830](#)
- PS/2 mouse, [334](#)
- PSU. *See* [power supply](#).
- public address, [1049](#)
- public cloud, [598](#)–599
- public/shared devices, [1092](#)–1093
- punch-down tool, [992](#), [1073](#)
- PuTTY, [1119](#)
- pwd command, [541](#)–542
- PXE (Preboot eXecution Environment), [82](#), [229](#), [610](#)

## Python script

- comment syntax symbol, [871](#)
- decision structures, [866](#)–867
- executing, [868](#)
- file, [830](#)
- loops, [867](#)–868
- overview, [865](#)–866
- variables, [866](#)

## Q

- QIC (quarter-inch cartridge) tape drives, [274](#)–275
- QoS (Quality of Service), [1021](#), [1138](#)
- QR (quick response) scanners, [412](#)
- quad-core processor, [144](#)
- quick format, [1169](#)

## R

- radio frequency, [1022](#)–1023, [1025](#)–1026
- radio frequency interference (RFI), [478](#)–479
- RADIUS, [1013](#), [1153](#)
- RAID (Redundant Array of Inexpensive Disks), [267](#)–269, [268](#), [275](#)–276, [1172](#)–1173
- RAID mode, [232](#), [266](#)
- Raid-5 volume, [795](#)
- rails, power supply, [285](#)
- rainbow tables, [1150](#)

RAM (random access memory)

- CMOS, [183](#)–184

- CMOS setup program settings, [219](#)

- compatibility, [199](#)

- overview, [79](#)

- slots, [95](#)–96

- static, [141](#)

- video, [85](#), [184](#), [351](#)

ransomware, [1155](#), [1238](#)

.rar file, [642](#)

rd (rmdir) command, [673](#)

RDP (Remote Desktop Protocol), [551](#), [600](#), [1063](#)

RDRAM (rambus DRAM), [185](#)–186

RE (Recovery Environment), [247](#)

Read permissions, [1207](#)

Read-only attribute, [646](#)–647

read/write head, [243](#)

read/write process, [245](#)

ReadyBoost, [528](#), [587](#)–588

reboots, [511](#)–513

recovery and rescue methods

- overview, [938](#)

- recovery DVDs, [938](#)

- recovery image, [939](#)

- recovery partitions, [938](#)

- rescue CDs, [939](#)–941

- rescue partitions (rescue installations), [943](#)

- USB drives, [938](#)

Recovery Console, [1247](#)

Recovery tab, [776](#)–777

Red Hat, [533](#)

reflective infrared, [379](#)

refresh rate, [353](#), [355](#), [584](#)

refresh/restore, [1247](#)

regedit.exe (Registry Editor), [666](#), [801](#)–806

Region and Language, Control Panel applet, [577](#)

registers, [140](#)–141

registration rollers, [370](#)

Registry, Windows

- boot process, [694](#)–696

- corruption if, [886](#)

- file associations, [635](#)–636

- overview, [571](#)–572

- subtrees, [801](#)

- Uninstall key, [730](#)

regsvr32.exe, [807](#)

regulated data, [1185](#)

- regulatory policy, [38](#)
- relative paths, [669](#)–672
- `rem` statements, [838](#)–839
- remote access, [1092](#)
- Remote Assistance, [582](#)–583, [1092](#)
- remote backup applications, [455](#)
- Remote Desktop Connection, [579](#), [580](#)–582, [1092](#)
- Remote Desktop Services, [775](#)
- remote disc, [550](#)
- remote wipes, [454](#)–455, [1182](#)
- RemoteApp, [579](#)
- removable storage
  - BD-R, [271](#)
  - BD-REs, [271](#)
  - Blu-Ray discs, [271](#)
  - CD-ROM/CD-RW, [269](#)–270
  - DVD/DVD-RW, [270](#)–271
  - flash drives/thumb drives, [272](#)
  - hybrid drives, [272](#)
  - M.2 SSDs, [274](#)
  - NVMe, [274](#)
  - overview, [269](#)
  - SD cards, [272](#)–274
  - SSDs, [271](#)
  - tape, [274](#)–275
- `ren` command, [677](#)
- renamed system files, [1245](#)

- repair installation, [619](#)
- repeaters, [980](#)–981
- rescue CDs, [939](#)–941
- rescue partitions (rescue installations), [943](#)
- reservations, [1049](#)
- reserve resources, [233](#)
- reset button, [94](#)
- resolution, [350](#), [355](#), [583](#)–584
- Resource Arbitrator, [717](#)
- Resource Monitor, [753](#)
- resource pooling, cloud, [596](#)
- respect, [48](#)–50
- restore point, [1249](#)
- retake policy, exams, [28](#)
- revision number, BIOS, [227](#)–228
- RFC (Request for Change), [41](#)
- RFC (Request for Comments), [1104](#)
- RG-6 cable, [966](#)
- rights, [1165](#), [1201](#)–1203
- RIMM (rambus inline memory module), [185](#)–186
- Ring 0 (kernel mode), [566](#)
- rings, [566](#)
- riser cards, [340](#)
- risk analysis, [42](#)
- RJ-45 connectors, [964](#)
- RJ-45 port, [108](#)–109
- rm command, [538](#)

- robocopy.exe command, [674](#)–675
- rogue antivirus, [1245](#)
- roller, [376](#)
- ROM (read-only memory)
  - BIOS chip, [101](#)
  - EEPROM, [181](#)–182
  - EPROM, [181](#)
  - flash, [212](#)
  - overview, [79](#), [181](#)–182
- root access, unauthorized, [460](#)
- root directories, [667](#)
- rootkit, [1154](#), [1239](#)
- Roshal Archive, [642](#)
- routers
  - basic settings, [1014](#)–1016
  - encryption, [1017](#)–1018
  - MAC filtering, [1018](#)–1019
  - overview, [982](#)
  - passwords, [1016](#)–1017, [1225](#)
  - security, [1016](#)–1020
  - for SOHO network, [1013](#)–1021, [1133](#)–1134
- RPM (Red Hat Package Manager), [533](#)
- RS-232 port. *See* [serial ports](#)
- RSI (repetitive strain injury), [69](#)
- runas command, [665](#)–666

## S

SaaS (Software as a Service), [601](#)

Safe Mode, [886](#)–887, [889](#), [920](#)–921

safety

- computer components, [63](#)–64

- electromagnetic interference, [60](#)–61

- electrostatic discharge, [58](#)–60

- environmental impacts and controls, [66](#)–68

- ergonomics, [69](#)–70

- high-voltage equipment, [62](#)

- personal, [61](#)–62

- Prep Test, [71](#)–73

- tools, [55](#)–58

- toxic waste, [64](#)–66

safety goggles, [62](#)

SAM (Security Accounts Manager) database, [1161](#)

Santayana, George (philosopher), [38](#)

Sarbanes- Oxley Act, [1174](#)

SAS (Serial Attached SCSI), [78](#), [118](#)

SATA (Serial Advanced Technology Attachment)

- cables, [318](#)–319

- cabling, [265](#)

- connectors, [265](#)–266

- general discussion, [264](#)–266

- overview, [78](#), [116](#)–117

- power connector, [291](#)

- versions, [266](#)

satellite Internet, [1130](#)



Scalable Vector Graphic, [643](#)

scanners

- connecting, [403](#)

- drum, [402](#)

- flatbed, [402](#)

- handheld, [402](#)

- overview, [338](#), [401](#)–402

- preventive maintenance, [486](#)–487

- QR (quick response), [412](#)

- scanning images, [403](#)–404

- scanning process, [403](#)

- sheetfeed, [402](#)

Scanners and Cameras, Control Panel applet, [577](#)

scatter infrared, [379](#)

scheduling, printer, [383](#)

SCP (Secure Copy Protocol), [1118](#)

screen

- calibration, [453](#)

- orientation, [453](#)

- resolutions, [85](#)–86

screen flicker, [505](#)

screen locks, [454](#), [1179](#)

Screen Sharing. Mac OS, [551](#)

screensaver, [1179](#)

screwdrivers, [56](#)

script.exe, [839](#)

## scripting

- adding comments to code, [870](#)

- batch files, [831](#)–839

- file types, [830](#)

- JavaScript, [868](#)–870

- overview, [829](#)–830

- PowerShell, [851](#)–862

- Prep Test, [872](#)–874

- Python, [865](#)–868

- Shell Script, [863](#)–865

- VBScript, [839](#)–851

## SCSI (Small Computer System Interface)

- adapter/card/controller, [117](#)–118, [255](#)–256

- addressing, [258](#)–259

- bus, [256](#)

- cabling, [260](#)

- daisy-chaining, [363](#)

- host adapter, [256](#)–258

- IDs, [258](#)–259

- installing devices, [263](#)–264

- overview, [78](#), [255](#)–256

- performance, [256](#)

- printers, [380](#)

- scanners, [403](#)

- terminators, [260](#)–261

- types of, [262](#)–263

## SCSI-1, [262](#)

SD (Secure Digital) cards, [272](#)–274

SDHC (Secure Digital High Capacity) cards, [273](#)

SDRAM (synchronous DRAM), [185](#)

SDXC (Secure Digital Extended Capacity) cards, [273](#)

searchable knowledge base, [38](#)

SEC (single edge contact) chip, [149](#), [156](#)

SECC (single edge contact connector), [156](#)

secondary corona wire, [372](#)

Secondary Logon, [775](#)

sector blocks, [243](#)–244

sectors, hard drive, [243](#)–244

secure boot, [225](#)–226

## security

attack types, [1146](#)–1156

auditing, [1212](#)–1215

authentication, [1159](#)–1164, [1193](#)

authorization, [1164](#)–1165

best practices, [1157](#)–1159, [1175](#)–1180, [1221](#)–1226

BIOS/UEFI, [222](#)–226, [1157](#), [1192](#)

browser settings, [1121](#)

data protection, [1167](#)–1175

digital, [1176](#)–1177

firewalls, [1215](#)–1221

incident response, [1182](#)–1185

macro security settings, [1232](#)–1233

mobile devices, [454](#)–456, [460](#)–462, [1182](#)

overview, [1145](#)

permissions, [1165](#), [1205](#)–1210

physical, [1156](#)–1159, [1175](#)–1176

port, [1194](#)

Prep Test, [1187](#)–1189, [1227](#)–1229

rights, [1165](#)

SOHO, [1016](#)–1019, [1135](#)–1136

of transmissions, [1166](#)–1167

user education, [1177](#)

wireless network, [1007](#)–1013, [1016](#)–1020, [1027](#), [1225](#)–1226

workstation, [1178](#)–1180

security alerts, [1245](#)

Security and Maintenance, [577](#)

- Security Center, [577](#), [775](#), [1221](#)
- security incident, [1183](#)
- security log, [1214](#)–1215
- Security+ certification, [7](#)
- seek time, hard drive, [245](#)
- Segus, Christopher, [940](#)
- self grounding, [60](#)
- Sempron processor (AMD), [165](#)
- serial cables
  - null modem cable, [314](#)–315
  - overview, [312](#)–313
  - standard, [313](#)–314
- serial connectors, [315](#)–317
- serial devices, [363](#)
- serial ports
  - CMOS setup program settings, [221](#)
  - on motherboard, [104](#)–105
  - overview, [86](#), [989](#)
  - troubleshooting, [506](#)–507
- Server Core Installation, [1119](#)
- server room, [1156](#)
- Server service, [1094](#)
- server-based (client-server) networks, [953](#)–955

## servers

- peer-to-peer (P2P) networks, [952](#)

- proxy, [1051](#)–1052

- roles, [955](#)

- security, [1157](#)

- SOHO, [1134](#)

service documentation, [39](#)

service load process, [695](#)

## services

- auto-restart issues, causing, [900](#)

- configuring, 090

- dependency, [910](#)

- DHCP, [1094](#)

- failing to start, [912](#)

- file-sharing, [1039](#), [1039](#)–1040

- incompatibility, [910](#)

- Messenger, [1095](#)

- optimization best practices, [774](#)–778

- overview, [1117](#)

- Print Spooler, [1094](#)

- printer sharing, [1039](#)

- restarting, [1093](#)–1094

- Server, [1094](#)

- versions of, 090

- Windows-specific problems, [897](#)–899

- Workstation, [1094](#)

Services Administrative tool (`services.msc`), [811](#)

Services tab, Task Manager, [757](#)

session hijacking, [1152](#)

settings

- backing up, [34](#)–35

- damaged, [911](#)

set-top box, [339](#)

setup.exe, [726](#)

sfc.exe (System File Checker), [686](#), [815](#)

SFTP (Secure FTP), [1064](#)

SFX v3.42, [293](#)

SGML (Standard Generalized Markup Language), [1105](#), [1114](#)–1115

SGRAM (synchronous graphics RAM), [351](#)

Shadow Copy, [588](#)

share name, [1076](#)

shared devices, [1092](#)–1093

shared folders, [1075](#)–1078, [1210](#)–1212

shares

- administrative, [1081](#)–1082, [1210](#)–1211

- configuring, [1211](#)

- connecting to, [1079](#)–1081

- creating, [1074](#)–1075

- enabling, [1074](#)–1075

- hidden, [1079](#)

- local, [1210](#)–1211

- multiple, [1079](#)

- troubleshooting, [990](#)

- user-level access control, [1075](#)

sheetfeed scanner, [402](#)

Shell (.sh) script

- comment syntax symbol, [871](#)

- decision structures, [864](#)

- executing, [865](#)

- file, [830](#)

- loops, [864](#)–865

- overview, [863](#)

- variables, [863](#)

shells, [1118](#)–1119

Shell/Terminal, macOS, [551](#)

shortcuts, corrupted, [910](#)–911

shorter probe, [63](#)

shoulder surfing, [1148](#)

shredder, [1168](#)

`shutdown.exe` command, [541](#), [679](#)–680

shutdowns, [511](#)–513, [914](#), [926](#)

side-by-side apps, [529](#)

signal drop, [1181](#)

signal quality, [971](#)

signature pads, [412](#)

signed drivers, [714](#)–715

SIM (System Image Manager), [622](#)–623

SIMMs (Single Inline-Memory Modules), [96](#)

simple volume, [795](#)

simplex, [987](#)

single sign-on, [1193](#)



- single variable type, [854](#)
- single-core processor, [143](#)–144
- single-factor authentication, [1013](#)
- single-sided memory, [194](#)
- .sit file, [642](#)
- 16:9 aspect ratio, [348](#)
- 16:10 aspect ratio, [348](#)
- 16-bit applications, [738](#)–739
- 64-bit applications, [735](#)–738
- 64-bit processor, [144](#)–145
- 64-bit OSes, [520](#)
- Slackware, [533](#)
- SLAs (service level agreements), [932](#)
- sleep mode, Windows, [423](#)–424, [578](#)
- slow performance, [1245](#)
- slow printing, [388](#)
- SLP (Service Location Protocol), [1063](#)
- S.M.A.R.T. (Self-Monitoring, Analysis and Reporting Technology), [484](#)
- smart batteries, [421](#)
- smart camera, [452](#)
- smart card reader, [340](#)
- smart cards, [1161](#), [1177](#)
- smart phones, [449](#)–451
- smart TV, [339](#)
- smartphones. *See also* [mobile devices](#)
- SMB (Server Message Blocks) protocol, [1063](#), [1064](#)
- SMF (single-mode fiber), [969](#)

- SmoothWall, [1138](#)
- SMTP (Simple Mail Transport Protocol), [1063](#), [1105](#), [1110](#), [1111](#)
- smurf attack, [1150](#)
- snap-ins, [580](#)
- snapshot, [550](#), [1247](#)
- SNMP (Simple Network Management Protocol), [484](#), [1063](#), [1064](#)
- social engineering attacks, [1146](#)–1148
- social media, [48](#)
- socket types, processor, [95](#), [150](#)–152, [166](#)
- SODIMMs (small outline dual inline memory modules), [188](#)–189, [200](#)–201, [418](#), [440](#)
- soft power support, [122](#)
- software
  - defined, [81](#)
  - for preventive maintenance, [472](#)–473
- software attacks, [1153](#)–1154
- software firewalls, [1218](#), [1248](#)
- SOHO (small office/home office) network
  - configuration settings, [1136](#)–1138
  - home routers, [1133](#)–1134
  - overview, [1013](#)–1014
  - router settings, [1013](#)–1016, [1019](#)–1021
  - security, [1135](#)–1136
  - security settings, [1016](#)–1019
  - servers, [1134](#)
  - wireless networking for, [1135](#)
- solenoids, printer, [375](#)

sound cards

- configuring, [361](#)–362

- installing, [360](#)–361

- integrated, [360](#)

- overview, [129](#), [359](#)–360

- PCIe, [360](#)

- types of, [360](#)

- USB, [360](#)

Sound Properties dialog box, [362](#)

South Bridge chip, [99](#)–100

spam, [1245](#)

spanned volume, [795](#)

S/PDIF (Sony/Philips Digital Interface Format), [504](#)

speaker port, [108](#)

speakers, [362](#), [447](#), [460](#)

speculative execution, [155](#)

speed

- CPU, [138](#), [219](#)

- memory, [198](#)

- network card, [1090](#)

- spin speed, hard drive, [246](#)

SpeedFan, [484](#)

spikes, [295](#)

spin speed, hard drive, [246](#)

spinning wait indicator, [493](#)

splitters, [971](#)

SPOD (Spinning Wheel of Death), [493](#)

spontaneous system restart/shutdown, [914](#)

spoofing, [1150](#)–1151

spooling, printer, [383](#), [388](#)–389

Spotlight, [549](#)

Spotlight, macOS, [549](#)

spots or smudging on printouts, [388](#)

Spybot Search & Destroy, [1237](#)

spyware, [1155](#), [1237](#)–1238

SQL injection, [1153](#)

SQL Slammer, [902](#)

SRAM (static RAM), [183](#)

SR-IOV passthrough, [593](#)

SSDs (solid-state drives), [77](#), [271](#), [439](#), [456](#), [500](#)–502, [772](#)

ssh (secure shell), [1119](#)

SSH (Secure Shell) protocol, [1062](#), [1064](#), [1092](#)

SSID (Service Set Identifier), [1002](#), [1008](#)–1009, [1014](#)–1015, [1019](#), [1027](#), [1225](#)–1226

SSL (Secure Sockets Layer), [1011](#), [1116](#)–1117, [1167](#)

SSO (single sign-on), [1163](#)

ST (straight tip) connector, [970](#)

standard user, [1199](#), [1206](#)

standby mode, [423](#)–424

standby UPS, [296](#)

star topology, [959](#)–960

Start menu, Windows, [580](#)

Start screen, Windows, [529](#), [580](#)

Startup Repair, [928](#)

- Startup tab, [758](#), [778](#)
- static configuration, [1045](#)–1049
- static RAM, [141](#)
- StickyKeys, [331](#)–332
- stop bits, [507](#)
- Stop errors, [904](#)–905
- storage, as basic computer function, [75](#)–76
- storage cards, [339](#)
- storage devices. *See also* [hard drives](#)
  - overview, [77](#)
  - Prep Test, [277](#)–279
  - removable storage, [269](#)–275
- storage media
  - labeling of, [484](#)
  - preventive maintenance, [483](#)–484
  - shelf life of, [485](#)
- storage pool, [798](#)
- Storage Spaces, [797](#)–799
- STP (shielded twisted pair) cable, [962](#)
- str variable type, [854](#)
- streaks, printer problem, [392](#)
- striped volume, [267](#), [795](#), [1173](#)
- strong password, [1163](#), [1177](#), [1178](#)
- Stuffilt file, [642](#)
- stylus, [435](#)
- su command, [543](#)
- subnet mask, [1043](#)–1044

- subprocedures, VBScript, [842](#)–843
- subroutines, VBScript, [842](#)–843
- subscriber connector, [970](#)
- `sudo` command, [543](#)
- SugarSync, [931](#)
- Super XGA, [347](#)
- superscalar design, [154](#)
- suppressors, [479](#)–480
- surge suppressor, [68](#), [296](#)
- SUS (Software Update Service), [1241](#)
- SUSE, [533](#)
- suspend mode, Windows, [423](#)–424, [578](#)
- .svg file, [643](#)
- SVGA (Super Video Graphics Array), [86](#), [304](#), [347](#)
- S-Video connector, [348](#)
- swap file, [567](#), [696](#)
- `switch` statement, [856](#)–857
- switch-based keyboards, [328](#)
- switches
  - for directories, [670](#)
  - for `dism.exe`, [679](#)
  - managed, [984](#)
  - overview, [984](#)
  - for `robocopy.exe`, [675](#)–676
  - security implementation, [1224](#)–1225
  - for `shutdown.exe`, [679](#)
  - unmanaged, [984](#)

- Symantec, [473](#)
- Sync, [455](#)
- Sync Center, [579](#)
- synchronization
  - apps, [458](#), [602](#)
  - data, [457](#)–458
- Sysinternals, [771](#)
- syslog server, [955](#)
- System, Control Panel applet, [578](#)
- System attribute, [646](#)–647, [656](#)
- system boards, [80](#). *See also* [motherboards](#)
- System Configuration (`msconfig.exe`), [799](#)–801, [1248](#)
- System DSN, [820](#)
- System File Checker (`sfc.exe`), [815](#)
- system file extensions, [641](#)–642
- system files, [585](#), [641](#), [1212](#), [1245](#)
- system folders, [1212](#)
- System Image Recovery, [931](#)
- System Information tool (`msinfo32.exe`), [811](#)–812
- system lockup, [907](#)–909
- System Managed Size, [770](#)
- system memory. *See* [memory](#)
- System Properties, [706](#)–708
- System Protection, [588](#)
- System Restore, [588](#), [792](#), [935](#)–937, [1247](#), [1248](#), [1249](#)
- system/application log errors, [1246](#)
- SystemRescueCD, [473](#)

# *T*

T1/T3 connections, [1130](#)

tablets, [66](#)

TACACS, [1013](#)

tailgating, [1156](#)

Tape archive files, [642](#)

tape drives, [274](#)–275

.tar file, [642](#)

Task Manager

- Applications tab, [757](#)

- Networking tab, [754](#)

- overview, [750](#)

- Performance tab, [751](#)–755

- Processes tab, [755](#)–757

- Services tab, [757](#)

- Startup tab, [758](#)

- Users tab, [757](#)

Task Scheduler, [775](#), [818](#)–819

Taskbar, [580](#)

Taskbar and Navigation, [578](#)

Taskbar and Start Menu, [578](#)

`taskkill.exe` command, [680](#)–681, [770](#)

`tasklist.exe` command, [680](#), [769](#)



TCP/IP (Transmission Control Protocol/Internet Protocol), [1060](#)–1061

- configuring, [1045](#)–1049

- default gateway, [1044](#)–1045

- IP address, [1041](#)–1043

- IPv4 versus IPv6, [1052](#)

- name resolution, [1053](#)–1061

- Network Address Translation, [1051](#)

- overview, [1038](#)–1039, [1040](#)–1041, [1105](#), [1108](#)–1109

- planning settings, [1061](#)

- port numbers, [1062](#), [1062](#)–1063

- protocols, [1062](#)–1064

- proxy server, [1051](#)–1052

- public/shared devices, [1093](#)

- settings, changing, [1085](#)–1086

- special addresses, [1049](#)–1050

- subnet mask versus CIDR, [1043](#)–1044

- troubleshooting utilities, [1064](#)–1071

- versus UDP, [1062](#)

TCPView, [902](#)

Telnet, [1063](#), [1092](#), [1119](#)

temperature

- control, [67](#)

- monitoring, [231](#)–232

- sensors, [170](#)

temporary files, [585](#), [644](#), [773](#)–774

10 Gbps Ethernet standards, [975](#)

10 Mbps Ethernet standards, [973](#)–974

- 10Base2, [973](#)
- 10Base5, [973](#)
- 10BaseFL, [973](#)
- 10BaseT, [973](#)
- terminal, [1247](#)
- Terminal Emulator, [536](#)
- Terminal Services, [775](#)
- terminators, [260](#)–261, [958](#)
- tethering, [453](#), [1132](#)
- text files, [644](#)
- TFX v2.52, [293](#)
- .tgz file, [642](#)
- thermal paste, [170](#)
- thermal printers, [375](#)
- thermal sensor, [146](#)
- thermal stress, [480](#)
- thick client, [556](#)
- Thicknet, [965](#)–966, [968](#)–969
- thin client, [556](#)
- Thinnet, [965](#)–967
- 32-bit applications, [734](#)–738
- 32-bit processor, [144](#)–145
- 32-bit OSES, [520](#)
- This PC window, [573](#)–574
- threads, [142](#)–143
- 3D Now!, [162](#)
- 3D printers, [376](#)

- 3G, [1024](#), [1131](#)
- throttling, [146](#)
- thumb drives, [272](#)
- Thunderbolt, [79](#), [308](#)
- Thunderbolt cards, [338](#)
- TIFF (Tagged Image File Format), [644](#)
- time, CMOS setup program settings, [222](#)
- Time Machine, [550](#)
- timelines, [48](#)
- timeout, [1179](#)
- TLDs (top-level domains), [1126](#)–1127
- TN (Twisted Nematic) displays, [354](#)
- ToggleKeys, [332](#)
- tokens, software, [1194](#)
- tone generator and probe, [992](#), [1073](#)
- toner cartridge, [370](#)
- toner kits, disposal of, [65](#)–66
- toner vacuum, [392](#)
- tools
  - hardware, [56](#)–57
  - overview, [55](#)–58
  - software, [57](#)
- topology, [957](#)
- touch pad, [338](#), [339](#), [433](#)–434, [483](#)
- touch panel displays, [430](#)
- touch screen, [338](#), [459](#), [483](#)
- touch stick, [434](#)–435

TouchFLO, [456](#)  
toxic waste, [64](#)–66  
TPM (Trusted Platform Module), [225](#), [1157](#), [1224](#)  
trace route (`tracert.exe`) utility, [1067](#)  
tracks, hard drive, [243](#)  
training, [40](#)  
transfer corona wire, [370](#), [372](#)  
transfer speeds, [991](#)  
transistor, [166](#), [169](#)  
transmissions, [1166](#)–1167  
Travan tape drives, [275](#)  
TRIM, [790](#)  
triple-channel memory architecture, [193](#)  
triple-core processor, [144](#)  
Trojan horses, [1154](#), [1236](#)

troubleshooting. *See also* [disaster recovery](#); [errors](#); [problems](#)

audio, [495](#)–497

audio problems, [504](#)

basic practices, [28](#)

cables, [970](#)–971

CMOS, BIOS, and UEFI, [497](#)–499

computer components, swapping, [492](#)

displays, [357](#)–359, [505](#)–506

error messages, [492](#)

escalation in, [36](#)

establishing theory of probable cause in, [33](#)

finding potential fixes in, [33](#)

hard drives, [275](#)–276, [500](#)–502

hypothesis evaluation/generation in, [30](#)

identifying problem, [31](#)–32

implementing preventive measures in, [37](#)

keyboard, [502](#)–503

laptops, [444](#)–448

layered or linear approach, [31](#)

log entries, [492](#)

mobile devices, [459](#)–460, [1181](#)–1182

motherboards, [498](#)

mouse, [502](#)–503

networking, [989](#)–992

optical drives, [502](#)

overview, [491](#)

physical environment, [494](#)

- POST errors, [495](#)–496
- power supplies and batteries, [509](#)–513
- Prep Test, [514](#)–516
- printers, [386](#)–394
- processor/memory, [498](#)–499
- projectors, [359](#)
- proprietary crash screens, [493](#)–494
- questioning the obvious in, [33](#)
- serial ports, [506](#)–507
- solid-state drives, [500](#)–502
- testing theory to determine cause in, [34](#)–36
- tools, [991](#)–992, [1072](#)–1073
- USB, [507](#)–509
- verifying full system functionality in, [37](#)
- visual, [495](#)–497
- Windows installations, [623](#)–624
- wireless networks, [1025](#)–1027
- Troubleshooting, Control Panel applet, [578](#)
- True Type font definition files, [643](#)
- trusted root CA, [1246](#)
- trusted software sources, [1177](#)
- .ttf file, [643](#)
- Turion 64 processor (AMD), [165](#)
- Turion 64 X2 processor (AMD), [165](#)
- TV tuners, [411](#)–412
- tvOS, [443](#)
- tweezers, [56](#)

12-volt power connector, [290](#)–291

twisted pair cabling, [962](#)–963

Type-A connector, [310](#)

Type-B connector, [310](#)

Type-C connector, [311](#)

## U

UAC (User Access Control), [527](#), [587](#), [1203](#)–1205

UAC Virtualization, [757](#)

Ubuntu Linux, [533](#), [884](#). *See also* [Linux OS](#)

UDMA (Ultra Dynamic Memory Access), [318](#)

UDP (User Datagram Protocol), [1062](#), [1108](#)

UEFI (Unified Extensible Firmware Interface)

- benefits of, [211](#)

- new and improved, [211](#)

- overview, [82](#), [211](#)

- passwords, [1179](#)

- physical security settings, [1157](#)

- securing system through, [1187](#)–1189

- troubleshooting, [497](#)–499

- Windows installations, [619](#)

Ultra SCSI, [262](#)

Ultra Wide SCSI, [262](#)

Ultra XGA, [347](#)

Ultra2 SCSI, [263](#)

unbuffered memory, [194](#)

UNC (universal naming convention), [1079](#), [1080](#)

unicast network traffic, [755](#)

Uninstall key, [730](#)

Unix OS, [532](#), [1109](#), [1118](#). *See also* [Linux OS](#)

unsigned drivers, [714](#)–715

updates

- automatic, [620](#)

- limitations, [554](#)

- macOS, [552](#)

- scheduling, [1249](#)

upgrading

- BIOS, [211](#)–214

- printer hardware, [380](#)–381

uploading pictures to computer, [406](#)

UPnP (Universal Plug and Play), [1021](#), [1137](#)

UPS (uninterruptible power supplies), [281](#), [295](#)–297, [479](#)–480

URL (Uniform Resource Locator), [1124](#)–1125



## USB (Universal Serial Bus)

cables, [310](#)–312, [458](#)

cards, [339](#)

CMOS setup program settings, [228](#)

expansion card, [130](#)

hubs, [110](#)

internal connectors, [109](#)–110

locks, [1162](#)

mouse, [334](#)

overview, [78](#)

ports, [86](#), [94](#), [109](#)–110

printers, [378](#)–379

recovery, [938](#)

scanners, [403](#)

sound cards, [360](#)

troubleshooting, [507](#)–509

user account database, [1160](#)

### user accounts

creating, [1195](#)–1198

description, [578](#)

details, [1196](#)

disabling, [1197](#)

full name, [1196](#)

passwords, [1196](#)–1197

standard, [1198](#)

user name, [1196](#)

user authentication, [1177](#)

User DSN, [820](#)  
user education, [1177](#)  
user files, [584](#)–585, [627](#)  
user limit, shared folder, [1076](#)  
user mode, [566](#)  
user password, [223](#)–225  
user rights, [1201](#)–1203  
user-level access control, [1074](#)  
usernames, [1111](#)  
users, [1199](#)  
USMT (User State Migration Tool), [588](#)  
UTM (Unified Threat Management), [956](#)  
UTP (unshielded twisted pair) cable, [962](#)–963  
Uencode, [642](#)  
UUID (universally unique identifier), [227](#)  
Unicode, [1109](#)

## V

vacuums, [68](#)  
vampire tap, [968](#)  
.vbs file, [640](#), [830](#)

## VBScript

- Boolean logic, [844](#)–845
- calling script, [839](#)–840
- comment syntax symbol, [871](#)
- decisions, [844](#)–845
- declarations, [840](#)–841
- external commands, [850](#)–851
- forcing a stop, [851](#)
- functions, [843](#)–844
- loops, [845](#)–847
- main procedure, [842](#)
- opening and saving files, [849](#)–850
- overview, [839](#)
- screen output, [847](#)–849
- script structure, [839](#)–844
- subprocedures, [842](#)–843
- subroutines, [842](#)–843
- working with parameters, [850](#)

vendor manuals, [39](#)

ventilation, [67](#), [473](#)–480, [496](#)

vertical line, printer problems, [391](#)

VGA (Video Graphics Array), [86](#), [304](#), [347](#)

VGA mode, [357](#)

VHD (Virtual Hard Disk) support, [528](#)

vi command, [545](#)–546

## video adapters/cards

- built-in coprocessors, [350](#)
- color depth, [85](#)
- installing, [351](#)–352
- laptop, [419](#)
- overview, [106](#), [345](#)–346
- resolution, [350](#)
- special connectors, [348](#)–349
- supported colors, [350](#)–351
- video memory, [351](#)

## video cables

- DisplayPort, [306](#)
- DVI, [306](#)–307
- HDMI, [305](#)
- mini-DisplayPort, [306](#)
- mini-HDMI, [305](#)
- overview, [304](#)
- VGA, [304](#)

## video capture cards, [411](#)–412

## video memory, [351](#)

## video port, [86](#)

## video standards, [347](#)

## virtual applications, [602](#)

## virtual desktops, [594](#)–595

## virtual device drivers, [643](#)

## virtual disk, [798](#)

## virtual memory, [562](#), [770](#)–772

- virtual printers, [375](#)–376
- virtualization, [144](#), [230](#)–231
- virtualization platforms, [590](#)–594
- virtualization workstation, [555](#)
- viruses. *See also* [malware](#) ([malicious software](#)).
  - antivirus software, [1234](#)–1235, [1242](#), [1246](#)
  - defined, [1231](#)
  - definitions, [1235](#)–1236
  - overview, [1154](#), [1231](#)
  - Prep Test, [1250](#)–1251
  - protection from, [1234](#)–1235
  - real-time protection from, [1235](#)
  - removing, [1244](#)–1246
  - types of, [1232](#)
  - virus protection settings, CMOS, [229](#), [230](#)
- Visual Basic Script file, [640](#), [830](#)
- Visual Effects, [780](#)
- VLANs (virtual LANs), [1052](#)–1053, [1225](#)
- VMM (Virtual Memory Manager), [567](#), [696](#)–699
- VMs (virtual machines), [230](#)–231, [600](#)
- VMXNNET 3, [593](#)–594
- VoIP (Voice over IP), [978](#)
- VoIP phones, [986](#)
- volt, [282](#)
- voltage, [232](#), [283](#)
- voltage power supplies, [284](#)
- Volume Shadow Copy, [775](#)

VPN (virtual private network), [600](#), [1011](#)–1012, [1091](#), [1167](#), [1177](#)  
VR (virtual reality) headsets, [412](#)  
VRAM (video RAM), [85](#), [184](#), [351](#)  
VRM (voltage regulator module), [146](#)  
VSS (Volume Shadow Copy Service), [588](#)  
vulnerability assessment software, [1242](#)  
.vxd file, [643](#)

## W

wake on LAN, [1090](#)  
WAN (wide area network), [956](#)–957, [1023](#)–1024  
WAN-cellular, [437](#)  
WAP (wireless access point), [960](#), [985](#)  
warm boot, [94](#)  
warm swapping, [717](#)  
warning lights, [496](#)  
watchOS, [443](#)  
watt, [282](#)–283  
WAV (Windows Audio files), [644](#)  
weak signal, [1181](#)  
wearable tech, [453](#)–454  
web cameras, [407](#)  
web pages, [1115](#)–1116  
website filters, [1134](#)  
websites, [1125](#)–1127  
WEP (Wired Equivalent Privacy), [1009](#)–1010, [1226](#)  
while loop, [845](#), [865](#), [868](#), [870](#)

- white stripes, printer problems, [391](#)
- white-hat hackers, [1146](#)
- whitelisting, [1137](#)
- Wide SCSI-2, [262](#)
- WiFi, [460](#), [1130](#)–1131, [1181](#)
- WIFI analyzer, [992](#)
- WiFiInfoView, [1026](#)
- wildcards, [536](#), [668](#)–669
- WiMax, [1133](#)
- WinAce file, [642](#)
- Window Maker, [533](#)
- Windows 3.0, [521](#)
- Windows 7
  - Backup and Restore tool, [931](#)
  - compatibility mode, [743](#)
  - editions, [522](#)
  - file and printer sharing in, [1074](#)
  - file names in, [634](#)
  - networking with, [1003](#)
  - special features, [527](#)–529
  - system requirements, [525](#)
  - themes, changing, [779](#)

## Windows 8.1

- applications, installing, [729](#)
- editions, [523](#)
- file and printer sharing in, [1074](#)
- networking with, [1003](#)
- special features, [529](#)–531
- startup settings, accessing, [924](#)–925
- system requirements, [525](#)

## Windows 10

- editions, [524](#)–525
- failure to boot recovery message, [927](#)
- file and printer sharing in, [1074](#)
- hardware requirements, [615](#)
- imaging with, [611](#)–613
- installing or removing additional components in, [626](#)–627
- networking with, [1003](#)
- special features, [532](#)
- startup settings, accessing, [924](#)–925
- system requirements, [525](#)
- themes, changing, [779](#)
- upgrading to, [625](#)

## Windows 9x family, [521](#)

## Windows Defender, [578](#), [1237](#)–1238

## Windows DVD, [57](#)

## Windows Error Recovery screen, [907](#)

## Windows Error Reporting Service, [775](#)

## Windows Event Log, [775](#)



Windows Explorer, [574](#)–575  
Windows Firewall, [578](#), [775](#)  
Windows Installer, [775](#)  
Windows keyboard, [329](#)  
Windows Live Sign-In, [530](#)  
Windows Managers, [533](#)  
Windows Memory Diagnostics, [815](#)–817  
Windows NT family, [521](#)

## Windows operating systems

- address space, [738](#)
- architecture, [566](#)–567
- attended installations, [620](#)–621
- boot process, [692](#)–696
- comparing versions of, [521](#)
- compatibility modes, [742](#)–743
- computer name, changing, [1054](#)–1055
- crash screens, [493](#)
- display settings, [583](#)–584
- families, [521](#)–525
- features of, [586](#)–590
- file systems, [617](#)–618
- file systems, choosing, [569](#)–570
- file types, [584](#)–586
- functions of, [562](#)–565
- GUI, [526](#)–532, [657](#)–658
- hardware requirements, [615](#)
- installation methods, [609](#)–614
- memory management in, [562](#)
- Microsoft Management Console, [579](#)–580
- mobile devices, [442](#)–443
- navigating computer with, [572](#)–576
- overview, [561](#)
- Prep Test, [605](#)–608, [629](#)–630
- Registry, [571](#)–572
- Remote Assistance, [582](#)–583

Remote Desktop Connection, [580](#)–582

shared folder, [1078](#)

system requirements, [525](#)–526

tools and configuration utilities, [576](#)

unattended installations, [622](#)

upgrading, [625](#)

version of, checking, [563](#)–565

virtual applications, [602](#)

virtual desktops, [594](#)–595

virtual memory, [567](#)–569

virtualization platforms, [590](#)–594

Windows PowerShell, [531](#), [576](#)

Windows Preinstallation Environment (PE), [612](#)–613

Windows Resource Monitor

CPU tab, [766](#)

Disk tab, [767](#)–768

Memory tab, [767](#)

Network tab, [768](#)

overview, [765](#)–768

Windows RT, [442](#)–443

Windows Search, [775](#), [780](#)–781

Windows Server 2008, [1119](#)

Windows Store, [531](#), [729](#)–730

Windows Update, [578](#), [944](#), [1240](#)

Windows Vista, [927](#), [1003](#), [1074](#)

Windows-based troubleshooting utilities. *See also* [configuration utilities](#)

configuration utilities, [799](#)–811

diagnostic utilities, [811](#)–817

disk maintenance, [786](#)–792

disk management, [793](#)–799

overview, [785](#)

Prep Test, [825](#)–827

WINE, [941](#)

winload.exe boot file, [882](#)

winload.exe command, [693](#)

WINS (Windows Internet Name Service), [1055](#)–1056

Winsock (Windows Socket), [1109](#)

WinVNC, [1092](#)

wire strippers, [1073](#)

wired connection, [1091](#)

wireless attacks, [1152](#)–1153

wireless connections, [459](#), [1130](#)–1131

wireless cut-off switch, [447](#)

wireless locator, [1073](#), [1091](#)

wireless mouse, [333](#)

wireless network card, [337](#), [436](#)

## wireless networking

ad hoc mode, [1001](#)

Bluetooth, [1021](#)–1022

clients, [1012](#)

components of, [1001](#)

connecting to network, [1002](#)–1003, [1091](#)

encryption, [1017](#)–1018

firmware, [1012](#)

infrared, [1000](#), [1022](#)–1023

infrastructure mode, [1001](#)–1002

issues in, [990](#)–991

near field communication, [1022](#)–1023

overview, [1000](#)–1001

passwords, [1000](#)

performance, increasing, [1024](#)–1025

Prep Test, [1027](#)–1030

protocols, [1004](#)–1007

radio frequency, [1022](#)–1023

security, [1007](#)–1013, [1027](#), [1225](#)–1226

for SOHO, [1013](#)–1021, [1135](#)

SSIDs, [1008](#)–1009

standards, [1004](#)–1007

troubleshooting, [1025](#)–1027

ZigBee, [1022](#)–1023

Z-Wave, [1022](#)–1023

wireless printers, [378](#)

wireless topology, [960](#)–961

- wiring standards, [963](#)–965
- WLAN Autoconfig, [775](#)
- WMN (wireless mesh network), [957](#)
- WoL (Wake on LAN), [426](#)
- workgroup, [616](#), [1054](#), [1084](#)–1085
- workstation
  - collision detection, [972](#)
  - multiple access, [972](#)
  - security, [1178](#)–1180
- Workstation service, [775](#), [1094](#)
- World Wide Web, [1114](#), [1127](#)
- WORM (write once read many) disc, [270](#)
- worms, [902](#), [1155](#), [1237](#)
- WoW (Windows on Windows), [738](#)–739
- WPA (WiFi Protected Access), [1010](#), [1226](#)
- WPA Enterprise, [1010](#)
- WPA Personal, [1010](#)
- WPA2 (802.11i), [1010](#)–1011, [1153](#), [1226](#)
- WPS (WiFi Protected Setup), [1021](#)
- WRAM (Window RAM), [351](#)
- wrist rest, [69](#)
- Write permission, [1207](#)
- wscript.exe, [839](#), [847](#)
- WSUS (Windows Server Update Services), [1241](#)
- WUXGA (Widescreen Ultra Extended Graphics Array), [347](#)
- WWAN (wireless WAN), [437](#), [1024](#), [1091](#)

## X

`xcopy` command, [674](#)–675  
xD (Extreme Digital) cards, [274](#)  
Xeon processors, [158](#)–159  
XGA (Extended Graphics Array), [304](#), [347](#)  
XHTML (Extensible Hypertext Markup Language), [1116](#)  
.xls file, [641](#)  
.xlsx file, [641](#)  
XML (Extensible Markup Language), [622](#), [1116](#)  
xml variable type, [854](#)  
XP Mode, [528](#)  
xterm, [536](#)  
XWindows, [533](#)

## Z

zero-day attack, [1153](#)  
ZIF (zero insertion force) socket, [95](#), [122](#), [147](#), [148](#), [167](#)–168  
ZigBee, [1022](#)–1023  
Zip drives, [248](#)  
.zip file, [642](#)  
zombie/botnet attack, [1153](#)  
zoom, [405](#)  
Z-Wave, [1022](#)–1023

# About the Authors

## **Glen E. Clarke**

**(MCSE/MCSD/MCDBA/CCNA/CEH/CHFI/Security+/Network+/A+)**

is owner of DC Advanced Technology Training (DCATT), a training and consulting company based out of Halifax, Nova Scotia. Glen spends most of his time delivering certified courses on A+, Network+, Windows Server, SQL Server, SharePoint, Exchange Server, .NET, Java, and Android programming. Glen also teaches a number of security-related courses covering topics such as ethical hacking and countermeasures, vulnerability testing, firewall design, and packet analysis.

Glen is an experienced author and technical editor who has worked on over 20 certification books. Glen designed and coauthored the award-nominated *A+ Certification Bible* and has worked on certification titles involving topics such as Windows certification, Cisco CCENT and CCNA certification, Network+ certification, and Security+ certification. Glen is author of the *CCENT Certification All-in-One For Dummies*, *CompTIA Security+ Certification Study Guide*, and *CompTIA Network+ Certification Study Guide*.

When he's not working, Glen loves to spend quality time with his wife, Tanya, and their four children, Sara, Brendon, Ashlyn, and Rebecca. You can visit Glen online at [www.glenclarke.com](http://www.glenclarke.com), or contact him at [glenclarke@dcatt.ca](mailto:glenclarke@dcatt.ca).

**Edward Tetz** graduated in 1990 from Saint Lawrence College in Cornwall, Ontario with a degree in Business Administration. Since that time he has spent his career delivering certified technical training for a Microsoft Training Center and working as a consultant for a Halifax, Nova Scotia based value-added reseller. While working as a consultant, he has supported Apple Macintosh, IBM OS/2, Linux, Novell NetWare, and all Microsoft operating systems from MS-DOS to Windows Server 2012, as well as hardware from most of the major manufacturers. This work was primarily focused around supporting enterprise and government



customers. He currently works for Microsoft in Enterprise Service Delivery in Ottawa, Ontario, still supporting similar customers.

Some of the certifications that he holds, or has held over the years, include A+, Cisco Certified Network Associate (CCNA), ITIL Foundations Certificate in IT Service Management (IT Infrastructure Library), Microsoft Certified Trainer (MCT), Microsoft Certified Systems Engineer (MCSE), Microsoft Certified Database Administrator (MCDBA), and Chauncey Group's Certified Technical Trainer (CTT).

When writing is not filling up his non-working hours, he enjoys spending time with his wife, Sharon, and their two girls, Emily and Mackenzie.

He welcomes comments from his readers and can be contacted at [ed\\_tetz@hotmail.com](mailto:ed_tetz@hotmail.com).

**Timothy Warner** is an IT professional, technical trainer, and author based in Nashville, Tennessee. Tim's been involved with computers in one way or another since 1982, when he received a Commodore 64 as a birthday present.

Tim considers himself an IT generalist because he enjoys practically every facet of information technology. Since entering the field in 1997, Tim worked a variety of job roles in the education and enterprise business sectors: PC repair technician, systems administrator, technology developer, and software architect.

Tim is a three-time Microsoft Most Valuable Professional (MVP) in Cloud and Datacenter Management, a Microsoft Certified Trainer (MCT), and holds over 50 IT certification titles, including, of course, the CompTIA A+.

When he's not working, Tim loves composing on his guitar (he lives in Music City, USA, after all), and spending time with his wife, Susan, and daughter, Zoey, and their animal menagerie. You can connect with Tim online at [TechTrainerTim.com](http://TechTrainerTim.com).

# *Dedications*

To my beautiful wife, Tanya, who has made all my dreams come true!

— Glen E. Clarke

I would like to dedicate this book to the love of my life, my wife, Sharon.

— Edward Tetz

To all my students, past, present, and future. I couldn't do what I do without you! Best of life to you in all your professional endeavors.

— Timothy Warner

# *Authors' Acknowledgments*

I want to thank the people at Wiley for their hard work and continued support. A special thank you to acquisitions editor, Ashley Coffey, for asking Ed, Tim, and me to do the fifth edition of this book. I thank her for her patience as I worked through the chapters of this book. A special thank you to Project Editor Katharine Dvorak for her patience and hard work keeping Ed, Tim, and me on track! I also want to thank Sean Wilkins for his feedback as the technical editor and a job well done!

Over the years I have developed friendships through my work, and one of my favorite people to work with is one of the coauthors of this book — Ed Tetz. We have worked together on many projects and I greatly appreciate his technical knowledge and willingness to help when I have a question. Thanks, Ed! A huge thanks to Timothy Warner for his hard work and dedication to another edition of the book and for helping us get the book completed in a timely fashion. I also want to thank the folks at Tim Horton's for not kicking me out when I occupy a table for hours at a time and for keeping the coffee *always fresh*!

A special thank you goes to my four children, Sara, Brendon, Ashlyn, and Rebecca, for giving me the time to sit down and participate in family time with them — it makes me realize what is important in life. A needed thank you goes to my wife, Tanya, for all her support — you are amazing! Thank you for all that you do!

— Glen E. Clarke

I would like to thank Ashley Coffey, our acquisitions editor, for inviting us to take on this project, and to both Ashley and Katharine Dvorak, our project editor, for keeping this book on track.

In addition to Ashley and Katharine, I would like to thank our technical editor, Sean Wilkins, as well as the rest of the staff at John Wiley & Sons, Inc., who worked behind the scenes taking care of many of the details that are required to get this book into print, and I am sure that due to their hard work, this will be a successful book.

— Edward Tetz

It's always been my dream to write a *For Dummies* book. Thanks to Ashley Coffey and Katharine Dvorak at Wiley for making it a reality. Thank you, Glen Clarke and Ed Tetz, for allowing me to join the team! Dave Dusthimer, thanks for being a mentor and teaching me more about CompTIA (the organization and its certs) than I ever thought possible.

— Timothy Warner

## **Publisher's Acknowledgments**

**Acquisitions Editor:** Ashley Coffey

**Project Editor:** Katharine Dvorak

**Technical Editor:** Sean Wilkins

**Proofreader:** Debbye Butler

**Sr. Editorial Assistant:** Matthew Lowe

**Production Editor:** Siddique Shaik

**Cover Image:** © a\_v\_d/Shutterstock

# Take Dummies with you everywhere you go!



Go to our [Website](#)



Like us on [Facebook](#)



Follow us on [Twitter](#)



Watch us on [YouTube](#)



Join us on [LinkedIn](#)



Pin us on [Pinterest](#)



Subscribe to our [newsletter](#)



Create your own [Dummies book cover](#)

**for  
dummies®**  
A Wiley Brand

# WILEY END USER LICENSE AGREEMENT

---

Go to [www.wiley.com/go/eula](http://www.wiley.com/go/eula) to access Wiley's ebook EULA.